thematics

MA

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel

H. Hasse L. Schlesinger

Wissenschaftlicher Beirat

H. Brandt / M. Dehn / G. Doetsch / A. Fraenkel / O. Haupt / F. Hausdorff
E. Hellinger / G. Kowalewski / H. Rademacher / K. Reidemeister
A. Rosenthal / C. Schaefer / W. Schmeidler / F. Schottky / O. Toeplitz

Band 169

Heft 3

Ausgegeben den 21. April 1933

D 19

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1933

Band 169. Heft 3.

Inhaltsverzeichnis.

	Seite
Vassiliou, Ph., Bestimmung der Führer der Verzweigungskörper relativ-abelscher Zahlkörper. Beweis der Produktformel für den Führer-Diskriminanten-Satz . .	131
Chevalley, Claude, La théorie du symbole de restes normiques	140
Davenport, H., On certain exponential sums	158
Haupt, Otto, Zur Differentialgeometrie der Kurven und Flächen	177
v. Sz. Nagy, Julius, Über einen Satz von Laguerre	186

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgend einem Grunde Text-Änderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion ausschließlich unter der Adresse:

An die Redaktion des Journals für die reine und angewandte Mathematik

Professor Dr. Kurt Hensel, Marburg-Lahn, Behringweg 7.

Bestimmung der Führer der Verzweigungskörper relativ-abelscher Zahlkörper. Beweis der Produktformel für den Führer-Diskriminanten-Satz*).

Von *Ph. Vassiliou* in Saloniki.

1. Der genaue Zusammenhang zwischen der Relativdiskriminante $\mathfrak{d}$ eines abelschen Körpers K/k und dem Führer $\mathfrak{f}$ der Idealgruppe, zu der dieser Körper als Klassenkörper gehört, wird bekanntlich durch die Formel

$$\mathfrak{d} = \prod_{\chi} \mathfrak{f}_\chi$$

geliefert, in der das Produkt auf der rechten Seite über alle sogen. χ-Führer erstreckt ist [1]). Diese Formel, welche zuerst aus der Funktionalgleichung der Heckeschen L-Reihen mit Größencharakteren gewonnen wurde, wurde später auf arithmetischem Wege von Hasse [2]) und unabhängig auch von Iyanaga [3]) bewiesen.

Die vorliegende Arbeit soll, vermittels eines Satzes von Herbrand, eine Vereinfachung der Untersuchungen von Hasse erzielen, die sich auf die Führer der verschiedenen Verzweigungskörper eines gegebenen Primideals $\mathfrak{p}$ des Grundkörpers für K/k beziehen. Dabei wird sich unmittelbar der explizite Ausdruck für den χ-Führer (s. u. § 11) ergeben, und damit dann ein neuer Beweis der oben angegebenen Produktformel des Führer-Diskriminanten-Satzes.

2. Bezeichnungen. K/k sei zunächst galoisch, $\mathfrak{G}$ seine galoissche Gruppe (K und k bedeuten algebraische Zahlkörper endlichen Grades). k'/k sei ein galoisscher Teilkörper von K, $\mathfrak{g}$ die Untergruppe von $\mathfrak{G}$, zu welcher dieser Körper im Sinne des Fundamentalsatzes der galoisschen Theorie gehört. $\mathfrak{P}$ bezeichne ein Primideal von K, $\mathfrak{p}'$ das durch $\mathfrak{P}$ teilbare Primideal von k'. Die $\mathfrak{P}$ bezüglich k bzw. k' als Grundkörper zugeordnete Hilbertsche Untergruppenreihe (Zerlegungsgruppe, Trägheitsgruppe, ..., ν-te Verzweigungsgruppe, ...) bezeichnen wir mit $\mathfrak{G}_Z, \mathfrak{G}_T, \ldots, \mathfrak{G}_\nu, \ldots$ bzw. $\mathfrak{g}_Z, \mathfrak{g}_T, \ldots, \mathfrak{g}_\nu, \ldots$ und die Ordnungen der Gruppen der letzteren Reihe mit $s_Z, s_T, \ldots, s'_\nu, \ldots$ Bekanntlich ist $\mathfrak{g}_Z = [\mathfrak{g}, \mathfrak{G}_Z]$, $\mathfrak{g}_T = [\mathfrak{g}, \mathfrak{G}_T], \ldots, \mathfrak{g}_\nu = [\mathfrak{g}, \mathfrak{G}_\nu], \ldots$, und die $s'_\nu = p^{f_\nu}$ sind Potenzen der durch $\mathfrak{P}$ teilbaren rationalen Primzahl p.

---

*) Für die freundliche Unterstützung beim Niederschreiben dieser Arbeit möchte ich Herrn H. Hasse an dieser Stelle meinen besonderen Dank aussprechen.

[1]) H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, Ia, II. Jahresber. D. M.-V. **35** (1926), **36** (1927), Erg. Bd. **6** (1930). Im folgenden zitiert mit „Hasse, Bericht I, Ia, II". — Siehe hierzu I, § 9. — Die Beiträge der unendlichen Primstellen zu $\mathfrak{f}$ und $\mathfrak{f}_\chi$ sind in diesem Zusammenhange außer Acht zu lassen.

[2]) H. Hasse, Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper. Journ. f. Math. **162** (1930). Im folgenden zitiert mit „Hasse, Führer". — Siehe auch Hasse, Bericht II, § 7.

[3]) S. Iyanaga, Über den Führer eines relativ zyklischen Zahlkörpers. Proc. Imp. Acad. Tokyo **5** (1929). — Siehe auch S. Iyanaga, Über den allgemeinen Hauptidealsatz. Japanese Journ. of Math. **7** (1930).

3. Die $\mathfrak{p}'$ bezüglich k als Grundkörper zugeordnete Hilbertsche Untergruppenreihe für k'/k bestimmt sich aus der $\mathfrak{P}$ für K/k zugeordneten nach dem in § 1 erwähnten Satz von Herbrand [4]). Zu seiner Formulierung bemerken wir noch folgendes: Die galoissche Gruppe des Körpers k'/k ist zur Faktorgruppe $\mathfrak{G}/\mathfrak{g}$ einstufig isomorph; dieser Isomorphismus kommt zustande, indem man jeder Nebengruppe aus der Faktorgruppe den durch ihre Elemente bewirkten Automorphismus von k'/k zuordnet; man kann daher diese Faktorgruppe selbst als die galoissche Gruppe von k'/k ansehen. Durch Bildung solcher Faktorgruppen, in dem eben angegebenen Sinne der Gleichheit, wird nun auch die gesuchte Untergruppenreihe geliefert. Bezeichnen γ_Z, $\gamma_T, \ldots, \gamma_\nu, \ldots$ die Faktorgruppen $\mathfrak{G}_Z\mathfrak{g}/\mathfrak{g}$, $\mathfrak{G}_T\mathfrak{g}/\mathfrak{g}, \ldots, \mathfrak{G}_\nu\mathfrak{g}/\mathfrak{g}, \ldots$, und $\mathfrak{g}'_Z$, $\mathfrak{g}'_T, \ldots, \mathfrak{g}'_\nu, \ldots$ die Hilbertschen Untergruppen von $\mathfrak{p}'$ für k'/k, so lautet der Herbrandsche Satz folgendermaßen:

Hilfssatz 1. *Man kann eine monoton wachsende Folge von Indizes* $1 \leqq h_1 < h_2 < \cdots$ *derart bestimmen, daß gilt:*

$$\begin{aligned} p^{s_1} + \cdots + p^{s_{h_1}} &= s_T \\ p^{s_{h_1+1}} + \cdots + p^{s_{h_2}} &= s_T \\ \cdots\cdots\cdots\cdots\cdots & \\ p^{s_{h_\varkappa+1}} + \cdots + p^{s_{h_\varkappa+1}} &= s_T . \end{aligned}$$

Für diese Einteilung gilt dann:

$$\begin{aligned} \gamma_1 = \gamma_2 = \cdots = \gamma_{h_1} &= \mathfrak{g}'_1 \\ \gamma_{h_1+1} = \gamma_{h_1+2} = \cdots = \gamma_{h_2} &= \mathfrak{g}'_2 \\ \cdots\cdots\cdots\cdots\cdots & \\ \gamma_{h_\varkappa+1} = \gamma_{h_\varkappa+2} = \cdots = \gamma_{h_{\varkappa+1}} &= \mathfrak{g}'_{\varkappa+1} . \end{aligned}$$

Außerdem ist

$$\gamma_Z = \mathfrak{g}'_Z, \quad \gamma_T = \mathfrak{g}'_T .$$

4. Es sei fortan K/k abelsch. $\mathfrak{p}$ sei das durch $\mathfrak{P}$ teilbare Primideal von k. K_ν $(\nu = 0, 1, \ldots, n;\ K_n = K)$ sei die aufsteigende Reihe der verschiedenen unter den Verzweigungskörpern (also K_ν der sogen. ν-mal überstrichene Verzweigungskörper), v_ν $(\nu = 1, \ldots, n)$ die zugeordneten Verzweigungszahlen. Die galoissche Gruppe von $K/K_{\nu-1}$, die wir weiterhin mit $\mathfrak{V}_\nu$ bezeichnen, ist dann die v_ν-te aber nicht die $v_\nu + 1$-te Verzweigungsgruppe im Sinne der früheren Abzählung.

Aus Hilfssatz 1 ergibt sich unmittelbar:

Satz 1. *Sind k', K' irgend zwei Körper mit der Eigenschaft*

$$K_{\nu-1} \leqq k' < K' \leqq K_\nu (\nu = 1, \ldots, n) ,$$

so ist für K'/k' zu jedem Primteiler von $\mathfrak{p}$ der Verzweigungskörper $K'_0 = k'$ und der einmal überstrichene Verzweigungskörper $K'_1 = K'$. Die zugehörige Verzweigungszahl ist $v'_1 = v_\nu$.

Entsprechend gilt auch:

Ist $K_T \leqq k' < K' \leqq K_0$ oder $k \leqq k' < K' \leqq K_T$, so ist für K'/k' zu jedem Primteiler von $\mathfrak{p}$ im ersteren Falle der Trägheitskörper $K'_T = k'$ und der Verzweigungskörper $K'_0 = K'$, im letzteren Falle der Trägheitskörper $K'_T = K'$.

Das sind die Sätze $\mathcal{U}'_\nu$, $\mathcal{U}'_0$, T' aus der Arbeit „Hasse, Führer".

5. Wir betrachten den ν-mal überstrichenen Verzweigungskörper über dem ν-1-mal überstrichenen, also $K_\nu/K_{\nu-1}$, und nennen den Relativgrad, der eine Potenz von p ist,

---

[4]) J. Herbrand, Détermination des groupes de ramification d'un corps à partir de ceux d'un sur-corps. Comptes rendus de l'Acad. Paris **191** (1930), p. 980. — Sur la théorie des groupes de décomposition, d'inertie et de ramification, Journ. de Math. **10** (1931).

p^{r_ν}. Die Faktorgruppe $\mathfrak{B}_\nu/\mathfrak{B}_{\nu+1}$ ist bekanntlich vom r_ν-gliedrigen Typus $(p, \ldots, p)$ [5]; dementsprechend kann K_ν als Kompositum von r_ν zueinander (bezüglich $K_{\nu-1}$) fremden zyklischen Körpern p-ten Grades über $K_{\nu-1}$ dargestellt werden. Für jeden dieser zyklischen Körper $K^*/K_{\nu-1}$ ist die Voraussetzung von Satz 1 erfüllt, und somit zu jedem Primteiler $\mathfrak{p}_{\nu-1}$ von $\mathfrak{p}$ in $K_{\nu-1}$ der Verzweigungskörper gleich $K_{\nu-1}$, der einmal überstrichene Verzweigungskörper gleich K^*, und die zu K^* gehörige Verzweigungszahl gleich v_ν. Der $\mathfrak{p}_{\nu-1}$-Führer von $K^*/K_{\nu-1}$ bestimmt sich demnach nach bekannten Sätzen der Klassenkörpertheorie [6]) zu

$$\mathfrak{f}_{\mathfrak{p}_{\nu-1}}(K^*/K_{\nu-1}) = \mathfrak{p}_{\nu-1}^{v_\nu+1}.$$

$K_\nu/K_{\nu-1}$ hat dann als Kompositum der K^* das kleinste gemeinsame Multiplum jener $\mathfrak{p}_{\nu-1}$-Führer zum $\mathfrak{p}_{\nu-1}$-Führer, d. h. es ist auch

$$\mathfrak{f}_{\mathfrak{p}_{\nu-1}}(K_\nu/K_{\nu-1}) = \mathfrak{p}_{\nu-1}^{v_\nu+1}. \tag{1}$$

6. Es seien jetzt k_1, k', K' irgend drei Teilkörper von K mit der Eigenschaft $K_T \leqq k_1 < k' < K'$. k'/k_1 sei vom Primzahlgrad q (gleich p oder verschieden von p). $\mathfrak{p}_1$ sei ein Primteiler von $\mathfrak{p}$ in k_1 und $\mathfrak{p}'$ ein Primteiler von $\mathfrak{p}_1$ in k'.

v sei die zu $\mathfrak{p}_1$ für k'/k_1 gehörige Verzweigungszahl; wir setzen dabei $v = 0$, wenn für k'/k_1 zu $\mathfrak{p}_1$ der Trägheitskörper gleich k_1 und der Verzweigungskörper gleich k' ist. Dann gilt:

Hilfssatz 2. *Ist*

$$\mathfrak{f}_{\mathfrak{p}'}(K'/k') = \mathfrak{p}'^{1+v+a} \text{ mit } a > 0,$$

so ist $a = lq$ *und*

$$\mathfrak{f}_{\mathfrak{p}_1}(K'/k_1) = \mathfrak{p}_1^{1+v+l}.$$

Beweis. Die in Rede stehenden Führerbeiträge sind die Führer der zugeordneten $\mathfrak{p}$-adischen Körper $\overline{K}'/\overline{k}'$ und $\overline{K}'/\overline{k}_1$ [7]). Daher wird der Beweis erbracht sein, wenn die folgenden drei Feststellungen gemacht sind:

a) Ist l durch $ql \leqq a < q(l+1)$ definiert, so ist jede Zahl $\overline{\beta}_1$ aus $\overline{k}_1$ mit der Kongruenzeigenschaft

$$\overline{\beta}_1 \equiv 1 \bmod. \mathfrak{p}_1^{1+v+l} \tag{2}$$

in der $\overline{K}'$ in $\overline{k}_1$ zugeordneten Zahlgruppe $\overline{H}(\overline{K}'/\overline{k}_1)$ enthalten.

b) Es ist $ql = a$.

c) Es gibt eine Zahl $\overline{\beta}_{01}$ in $\overline{k}_1$ mit der Kongruenzeigenschaft

$$\overline{\beta}_{01} \equiv 1 \bmod. \mathfrak{p}_1^{1+v+(l-1)}, \tag{3}$$

die nicht in $\overline{H}(\overline{K}'/\overline{k}_1)$ enthalten ist.

Ad a). Aus der Kongruenz (2) folgt jedenfalls $\overline{\beta}_1 \equiv 1 \bmod. \mathfrak{p}_1^{1+v}$. Weil $\mathfrak{f}_{\mathfrak{p}_1}(\overline{k}'/\overline{k}_1) = \mathfrak{p}_1^{1+v}$ ist, liegt also $\overline{\beta}_1$ in $\overline{H}(\overline{k}'/\overline{k}_1)$, d. h. ist $\mathfrak{p}$-adische Norm einer Zahl $\overline{\beta}'$ aus $\overline{k}'$:

$$\overline{\beta}_1 = N(\overline{\beta}').$$

$N(\,)$ bezeichnet hier und im folgenden die Norm für $\overline{k}'/\overline{k}_1$.

Für diese Zahl $\overline{\beta}'$ gilt dann nach (2)

$$N(\overline{\beta}') \equiv 1 \bmod. \mathfrak{p}_1^{1+v+l}, \text{ d. h. mod. } \mathfrak{p}'^{qv+q(l+1)}.$$

---

[5]) Hasse, Bericht Ia, § 8, (8.).
[6]) Hasse, Bericht Ia, §§ 9, 17, 18.
[7]) Hasse, Bericht II, § 7, X.

Nach einem Satz von Takagi [8]) folgt daraus

$$\bar{\beta}' \equiv \bar{\alpha}'^{1-S} \bmod. \ \mathfrak{p}'^{v+q(l+1)},$$

wo S einen erzeugenden Automorphismus des zyklischen Körpers k'/k_1 bezeichnet, und $\bar{\alpha}'$ eine Zahl aus $\bar{k}'$ ist. Wegen $a < q(l+1)$, d. h. $a+1 \leqq q(l+1)$, gilt sicherlich erst recht

$$\bar{\beta}' \equiv \bar{\alpha}'^{1-S} \bmod. \ \mathfrak{p}'^{v+a+1},$$

und dies bedeutet, daß $\frac{\bar{\beta}'}{\bar{\alpha}'^{1-S}}$ in $\bar{H}(\bar{K}'/\bar{k}')$ enthalten ist. $N\left(\frac{\bar{\beta}'}{\bar{\alpha}'^{1-S}}\right) = N(\bar{\beta}') = \bar{\beta}_1$ liegt also in $\bar{H}(\bar{K}'/\bar{k}_1)$.

Ad b). Weil $\mathfrak{f}_{\mathfrak{p}'}(K'/k') = \mathfrak{p}'^{1+v+a}$ ist, gibt es ein $\bar{\beta}_0'$ in $\bar{k}'$ mit der Kongruenzeigenschaft

$$\bar{\beta}_0' \equiv 1 \bmod. \ \mathfrak{p}'^{1+v+(a-1)}, \tag{4}$$

das nicht in $\bar{H}(\bar{K}'/\bar{k}')$ enthalten ist.

Wäre nun $ql < a$, d. h. $ql \leqq a-1$, so folgte

$$\bar{\beta}_0' \equiv 1 \bmod. \ \mathfrak{p}'^{1+v+ql},$$

und daraus weiter [9])

$$N(\bar{\beta}_0') \equiv 1 \bmod. \ \mathfrak{p}'^{1+v+l}.$$

Nach (2) wäre dann $N(\bar{\beta}_0')$ in $\bar{H}(\bar{K}'/\bar{k}_1)$ enthalten, also $\bar{\beta}_0' \bar{\alpha}_0'^{1-S}$ mit einer geeigneten Zahl $\bar{\alpha}_0'$ aus $\bar{k}'$ in $\bar{H}(\bar{K}'/\bar{k}')$ enthalten [10]), und also auch $\bar{\beta}_0'$ selbst in $\bar{H}(\bar{K}'/\bar{k}')$ enthalten [11]). Das widerspricht aber der obigen Auswahl von $\bar{\beta}_0'$.

Ad c). Für die eben benutzte Zahl $\bar{\beta}_0'$ ist wegen $q(l-1) < a-1$ nach (4) sicherlich

$$\bar{\beta}_0' \equiv 1 \bmod. \ \mathfrak{p}'^{1+v+q(l-1)},$$

also wie eben wiederum

$$\bar{\beta}_{01} = N(\bar{\beta}_0') \equiv 1 \bmod. \ \mathfrak{p}'^{1+v+(l-1)}.$$

Diese Zahl $\bar{\beta}_{01}$ aus $\bar{k}_1$ hat somit die Kongruenzeigenschaft (3).

$\bar{\beta}_{01}$ ist ferner nicht in $\bar{H}(\bar{K}'/\bar{k}_1)$ enthalten; denn sonst wäre wiederum wie eben $\bar{\beta}_0'$ in $\bar{H}(\bar{K}'/\bar{k}')$ enthalten.

Damit ist Hilfssatz 2 bewiesen.

Im Falle, daß k' der Trägheitskörper des Primideals $\mathfrak{p}_1$ für k'/k ist, hat man weiter, daß die Exponenten von $\mathfrak{p}'$ in $\mathfrak{f}_{\mathfrak{p}'}(K'/k')$ und $\mathfrak{p}_1$ in $\mathfrak{f}_{\mathfrak{p}_1}(K'/k_1)$ einander gleich sind. Das ergibt sich für den Fall, daß k' sogar der Zerlegungskörper von $\mathfrak{p}_1$ für k'/k_1 ist, unmittelbar aus dem oben in [7]) zitierten Satz des Hasseschen Berichts, im anderen Falle nach denselben Schlüssen wie eben unter Anwendung der entsprechenden Relationen aus der Takagischen Geschlechtertheorie [12]).

---

[8]) T. Takagi, Über eine Theorie des relativ-Abelschen Zahlkörpers. Journ. of the Coll. of Science Tokyo **41** (1920), § 14. — Siehe auch Hasse, Führer, § 4, Rel. II_2, II_3. — Es sei hierzu bemerkt, daß der Beweis ebensogut mit alleiniger Benutzung der Takagischen Geschlechtertheorie (a. a. O. § 14), ohne den Übergang zu den $\mathfrak{p}$-adischen Körpern, erbracht werden kann.

[9]) Siehe Takagi, a. a. O. § 14, oder Hasse, Führer, § 4, Rel. I_2, I_3.

[10]) D. Hilbert, „Zahlbericht", Satz 90.

[11]) H. Hasse, Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen. Journ. f. Math. **162** (1930), Satz 5.

[12]) Takagi, a. a. O. § 14, oder Hasse, Führer § 4, Rel. I_1, II_1.

7. Wir suchen jetzt den $\mathfrak{p}$-Führer $\mathfrak{f}_\mathfrak{p}(K_\nu/k)$ $(\nu = 0, 1, \ldots, n)$ zu ermitteln. Nach (1) ist uns der $\mathfrak{p}_{\nu-1}$-Führer von $K_\nu/K_{\nu-1}$ $(\nu = 1, \ldots, n;\ \mathfrak{p}_{\nu-1}$ in $K_{\nu-1})$ bekannt. Der Übergang von $K_{\nu-1}$ zu k wird vermöge unseres Hilfssatzes 2 in einzelnen Schritten von Primzahlsprung über geeignete Zwischenkörper vollzogen. Dabei wird doppelte vollständige Induktion angewandt.

Es bezeichne, wie schon oben, p^{r_ν} den Grad von $K_\nu/K_{\nu-1}$, ferner e_0 den (zu p primen) Grad von K_0/K_T. Weiter bezeichne allgemein Exp. $\mathfrak{f}_\mathfrak{p}(K'/k')$ den Exponenten des $\mathfrak{p}'$-Führers von K'/k' für die Primteiler $\mathfrak{p}'$ von $\mathfrak{p}$ in k'. Dann gilt:

Satz 2. *Es ist*

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_\nu/k) = 1 + a_\nu = 1 + \frac{v_1}{e_0} + \frac{v_2 - v_1}{e_0 p^{r_1}} + \cdots + \frac{v_\nu - v_{\nu-1}}{e_0 p^{r_1 + \cdots + r_{\nu-1}}}.$$

Beweis. Wir setzen $K_T = K_{-1}$, bezeichnen mit r_0 die Anzahl der in e_0 aufgehenden Primfaktoren q, und rechnen $v = 0$ als Verzweigungszahl für K_0 (vgl. § 6). Wir schalten zwischen K_h und K_{h-1} $(h = 0, 1, \ldots, \nu - 1)$ eine Körperkette

$$K_{h-1} = k_{h,r_h} < k_{h,r_h-1} < \cdots < k_{h,1} < K_h$$

ein, bei der jeder Körper über dem vorhergehenden zyklisch von Primzahlgrad ist.

a) Es werde nun angenommen, daß für ein festes i mit $1 \leqq i < r_h$ bereits bewiesen ist:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_\nu/k_{h,i}) = 1 + v_h + \frac{v_{h+1} - v_h}{p^i} + \frac{v_{h+2} - v_{h+1}}{p^{r_h+1+i}} + \cdots + \frac{v_\nu - v_{\nu-1}}{p^{r_{\nu-1} + \cdots + r_{h+1} + i}}.$$

Für K_ν, $k_{h,i}$, $k_{h,i+1}$ liegt dann die Situation des Hilfssatzes 2 vor. Da nach Satz 1 Exp. $\mathfrak{f}_\mathfrak{p}(k_{h,i}/k_{h,i+1}) = 1 + v_h$ ist, so ist das im Hilfssatz 2 vorkommende

$$a = \frac{v_{h+1} - v_h}{p^i} + \cdots > 0.$$

Daher ist Hilfssatz 2 anwendbar. Er liefert:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_\nu/k_{h,i+1}) = 1 + v_h + \frac{a}{p}$$

$$= 1 + v_h + \frac{v_{h+1} - v_h}{p^{i+1}} + \cdots + \frac{v_\nu - v_{\nu-1}}{p^{r_{\nu-1} + \cdots + r_{h+1} + (i+1)}}.$$

Dabei ist zunächst $h > 0$ angenommen. Für $h = 0$ gilt Entsprechendes, wenn man an die Stelle von p^i das Produkt der i Primzahlen q setzt, die den Grad von $K_0/k_{0,i}$ ausmachen.

b) Es werde ferner angenommen, daß für ein festes h mit $-1 < h \leqq \nu - 1$ bereits bewiesen ist:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_\nu/K_h) = 1 + v_{h+1} + \frac{v_{h+2} - v_{h+1}}{p^{r_h+1}} + \cdots + \frac{v_\nu - v_{\nu-1}}{p^{r_{\nu-1} + \cdots + r_{h+1}}}.$$

Für K_ν, K_h, $k_{h,1}$ liegt dann ebenfalls die Situation des Hilfssatzes 2 vor. Da nach Satz 1 Exp. $\mathfrak{f}_\mathfrak{p}(K_h/k_{h,1}) = 1 + v_h$ ist, so ist das in Hilfssatz 2 vorkommende

$$a = v_{h+1} - v_h + \frac{v_{h+2} - v_{h+1}}{p^{r_h+1}} + \cdots > 0.$$

Daher ist Hilfssatz 2 anwendbar. Er ergibt:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_\nu/k_{h,1}) = 1 + v_h + \frac{a}{p}$$

$$= 1 + v_h + \frac{v_{h+1} - v_h}{p^1} + \frac{v_{h+2} - v_{h+1}}{p^{r_h+1+1}} + \cdots + \frac{v_\nu - v_{\nu-1}}{p^{r_{\nu-1} + \cdots + r_{h+1} + 1}}.$$

Das letztere liefert uns die Ausgangsfeststellung für den unter a) angelegten Induktionsschluß. Läßt man diesen ablaufen, so ergibt sich demgemäß:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_\nu/K_{h-1}) = 1 + v_h + \frac{v_{h+1} - v_h}{p^{r_h}} + \cdots + \frac{v_\nu - v_{\nu-1}}{p^{r_{\nu-1}+\cdots+r_h}}.$$

Für den in b) angelegten Induktionsschluß ist nun die Ausgangsfeststellung ($h = \nu - 1$) nach Satz 1 richtig. Läßt man demnach jetzt diesen zweiten Induktionsschluß ablaufen und beachtet das am Ende von § 6 Gesagte, so ergibt sich der behauptete Satz.

8. Der Beweis von Satz 2 ergibt insbesondere die Ganzzahligkeit der durch die sukzessive Anwendung von Hilfssatz 2 auftretenden Brüche, d. h. die Kongruenzen:

$$v_1 \equiv 0 \text{ mod. } e_0$$
$$v_\nu \equiv v_{\nu-1} \text{ mod. } e_0\, p^{r_1+\cdots+r_{\nu-1}} \qquad (\nu = 2, \ldots, n).$$

9. Charakterisierung der Verzweigungskörper. Wir werden jetzt folgende Charakterisierung der Verzweigungskörper $K_\nu (\nu = 0, 1, \ldots, n)$ beweisen:

Satz 3. *Der ν-mal überstrichene Verzweigungskörper K_ν enthält alle Teilkörper von K/k, deren $\mathfrak{p}$-Führer höchstens $\mathfrak{p}^{1+a_\nu}$ ist.*

Er selbst hat, wie bereits bewiesen, den $\mathfrak{p}$-Führer $\mathfrak{p}^{1+a_\nu}$.

Beweis. Es sei K^* irgendein Teilkörper von K, der nicht in K_ν enthalten ist. Dann ist das Kompositum K^*K_ν ein echter Oberkörper K_ν.

Nach dem Herbrandschen Satze (Hilfssatz 1) stimmt die Reihe der überstrichenen Verzweigungskörper und der Verzweigungszahlen von $K^*\,K_\nu/k$ bis zu K_ν und v_ν hin mit der von K/k überein. Durch Anwendung des zuvor bewiesenen Satzes 2 auf K^*K_ν (als letzten seiner eigenen Verzweigungskörper) anstelle von K_ν ergibt sich dann, daß $\mathfrak{f}_\mathfrak{p}(K^*K_\nu/k) > \mathfrak{f}_\mathfrak{p}(K_\nu/k)$ ist. Bekanntlich ist aber

$$\mathfrak{f}_\mathfrak{p}(K^*K_\nu/k) = \text{Max. } (\mathfrak{f}_\mathfrak{p}(K^*/k), \mathfrak{f}_\mathfrak{p}(K_\nu/k)).$$

Daher ergibt sich weiter $\mathfrak{f}_\mathfrak{p}(K^*/k) > \mathfrak{f}_\mathfrak{p}(K/k)$, was den Beweis unseres Satzes erbringt.

10. Expliziter Ausdruck für den χ-Führer. Beweis der Produktformel für den Führer-Diskriminanten-Satz. Die Bestimmung der Führer der Verzweigungskörper ermöglicht es uns, den expliziten Ausdruck für den χ-Führer anzugeben und auf diese Weise den Beweis der Produktformel des Führer-Diskriminanten-Satzes zu gewinnen.

Es sei χ irgendein Charakter der Klassengruppe nach $H(K/k)$ in k, zu der K als Klassenkörper gehört. Wegen des Isomorphiesatzes der Klassenkörpertheorie ist χ auch Charakter der galoisschen Gruppe $\mathfrak{G}$ von K/k, wenn man festsetzt, daß für homologe Elemente beider Gruppen χ denselben Wert haben soll. $\mathfrak{f}_\chi = \mathfrak{f}(\chi, K/k)$ ist alsdann definiert als der Führer derjenigen Idealgruppe $H(\chi) = H(\chi, K/k)$ in k, welche sich aus allen Klassen nach $H(K/k)$ zusammensetzt, für die χ den Wert 1 hat. Zugehöriger Klassenkörper $K(\chi)$ zu dieser Idealgruppe $H(\chi)$ ist ersichtlich derjenige Zwischenkörper, welcher nach dem Fundamentalsatz der galoisschen Theorie der Untergruppe aller Elemente von $\mathfrak{G}$ mit dem χ-Wert 1 zugeordnet ist.

11. χ induziert für jede Untergruppe $\mathfrak{V}$ von $\mathfrak{G}$ wieder einen Charakter, den wir ebenfalls mit χ bezeichnen, da daraus keine Mißverständnisse zu befürchten sind. Es bedeute ferner $\chi(\mathfrak{V})$ die Summe der χ-Werte für alle Elemente von $\mathfrak{V}$.

Wir wenden vollständige Induktion an.

Induziert χ nicht den Hauptcharakter von $\mathfrak{V}_n$ (siehe § 4), so ist der Klassenkörper zu $H(\chi, K/K_{n-1})$, d. i. das Kompositum $\overline{K}_{n-1} = K(\chi)K_{n-1}$, nach dem oben Gesagten ein echter Oberkörper von K_{n-1}. Nach Formel (1) ist daher sein $\mathfrak{p}_{n-1}$-Führer gleich $\mathfrak{p}_{n-1}^{1+v_n}$.

Induziert dagegen χ den Hauptcharakter von $\mathfrak{B}_n$, so ist $H(\chi, K/K_{n-1})$ die Gruppe *aller* Idealklassen nach $H(K/K_{n-1})$, also jener $\mathfrak{p}_{n-1}$-Führer gleich $\mathfrak{p}_{n-1}^0$. In beiden Fällen ist also

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/K_{n-1}) = (1 + v_n)\frac{p^{r_n} - \chi(\mathfrak{B}_n)}{p^{r_n}} = \frac{1}{p^{r_n}}\left(p^{r_n} - \chi(\mathfrak{B}_n) + v_n(p^{r_n} - \chi(\mathfrak{B}_n))\right);$$

denn bekanntlich ist $\chi(\mathfrak{B}_n) = p^{r_n}$ oder 0, je nachdem χ der Hauptcharakter oder ein vom Hauptcharakter verschiedener Charakter von $\mathfrak{B}_n$ ist, und folglich ist der im Exponenten hinzugefügte Faktor $\dfrac{p^{r_n} - \chi(\mathfrak{B}_n)}{p^{r_n}} = 1$ oder 0, je nachdem der erste oder zweite der oben unterschiedenen Fälle vorliegt.

Es werde nun ferner schon als bewiesen angenommen, daß für ein festes i mit $1 \leqq i < n$ gilt:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/K_i) = \frac{1}{p^{R_{i+1}}}\Big(p^{R_{i+1}} - \chi(\mathfrak{B}_{i+1}) + v_{i+1}(p^{R_{i+1}} - \chi(\mathfrak{B}_{i+1}))$$
$$+ (v_{i+2} - v_{i+1})(p^{R_{i+2}} - \chi(\mathfrak{B}_{i+2})) + \cdots + (v_n - v_{n-1})(p^{R_n} - \chi(\mathfrak{B}_n))\Big),$$

wo $r_h = R_h - R_{h-1}$, $r_n = R_n$, d. h. $R_h = p^{r_h + r_{h+1} + \cdots + r_n}$ gesetzt worden ist.

Ist dieser Exponent, der zur Abkürzung mit c bezeichnet werden möge, $\neq 0$, d. h. $\chi(\mathfrak{B}_{i+1}) \not\equiv p^{R_{i+1}}$, so induziert also χ nicht den Hauptcharakter für $\mathfrak{B}_{i+1}$. Dann ist der Klassenkörper zu $H(\chi, K/K_i)$, d. i. das Kompositum $\bar{K}_i = K(\chi)K_i$ ein echter Oberkörper von K_i. Nach Satz 2, und unter Anwendung des Herbrandschen Satzes (Hilfssatz 1) ähnlich wie im Beweis zu Satz 3, folgt dann $c > 1 + v_i$ und

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\bar{K}_i/K_{i-1}) = 1 + v_i + \frac{c - (1 + v_i)}{p^{r_i}} = \frac{1}{p^{r_i}}\left(c + (p^{r_i} - 1)(1 + v_i)\right).$$

Wegen $\bar{K}_i = K_i\bar{K}_{i-1}$ ist aber

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\bar{K}_i/K_{i-1}) = \text{Max.}(\text{Exp. } \mathfrak{f}_\mathfrak{p}(K_i/K_{i-1}),\ \text{Exp. } \mathfrak{f}_\mathfrak{p}(\bar{K}_{i-1}/K_{i-1}))$$
$$= \text{Max.}(1 + v_i,\ \text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/K_{i-1})).$$

Unter Beachtung von $c > 1 + v_i$ folgt daraus, daß auch

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/K_{i-1}) = \frac{1}{p^{r_i}}\left(c + (p^{r_i} - 1)(1 + v_i)\right)$$

ist.

Ist aber $c = 0$, d. h. $\chi(\mathfrak{B}_{i+1}) = p^{R_{i+1}}$, so induziert also χ den Hauptcharakter von $\mathfrak{B}_{i+1}$, und es ist demnach $\bar{K}_i = K_i$. Entweder ist dann χ auch der Hauptcharakter für $\mathfrak{B}_i$, d. h. $\chi(\mathfrak{B}_i) = p^{R_i}$; dann ist $\bar{K}_{i-1} = K_{i-1}$, und folglich der Führerexponent von $H(\chi, K/K_{i-1})$ gleich 0. Oder es ist χ nicht der Hauptcharakter für $\mathfrak{B}_i$, d. h. $\chi(\mathfrak{B}_i) \not\equiv p^{R_i}$; dann ist $\bar{K}_{i-1}$ ein echter, in K_i enthaltener Oberkörper von K_{i-1}, und folglich der Führerexponent von $H(\chi, K/K_{i-1})$ nach Formel (1) gleich $1 + v_i$.

Alle drei Fälle lassen sich in der einen Formel zusammenfassen:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/K_{i-1}) = \frac{1}{p^{r_i}}\left(c + \frac{1}{p^{R_{i+1}}}\left((p^{R_i} - p^{R_{i+1}}) - (\chi(\mathfrak{B}_i) - \chi(\mathfrak{B}_{i+1}))(1 + v_i)\right)\right).$$

Setzt man hier den Wert von c ein, so ergibt sich nach leichter Umformung:

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/K_{i-1})$$
$$= \frac{1}{p^{R_i}}\left(p^{R_i} - \chi(\mathfrak{B}_i) + v_i(p^{R_i} - \chi(\mathfrak{B}_i)) + (v_{i+1} - v_i)(p^{R_{i+1}} - \chi(\mathfrak{B}_{i+1})) + \cdots\right).$$

Das macht die Induktion vollständig.

Vollzieht man schließlich den Übergang zu k selbst als Grundkörper unter Beachtung des am Ende von § 6 Gesagten, so ergibt sich die gesuchte Formel [13]):

$$\text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/k)$$
$$= \frac{1}{e_0 p^{R_1}} (e_0 p^{R_1} - \chi(\mathfrak{V}_0) + v_1(p^{R_1} - \chi(\mathfrak{V}_1)) + (v_2 - v_1)(p^{R_2} - \chi(\mathfrak{V}_2)) + \cdots).$$

Diese Formel kann auch so geschrieben werden:

$$\text{(5)} \quad \text{Exp. } \mathfrak{f}_\mathfrak{p}(\chi, K/k) = \frac{e_0 p^{R_1} - \chi(\mathfrak{V}_0)}{e_0 p^{R_1}} + \frac{v_1}{e_0} \frac{p^{R_1} - \chi(\mathfrak{V}_1)}{p^{R_1}} + \frac{v_2 - v_1}{e_0 p^{r_1}} \frac{p^{R_2} - \chi(\mathfrak{V}_2)}{p^{R_2}} + \cdots,$$

wo die Faktoren $\varepsilon_i = \dfrac{p^{Ri} - \chi(\mathfrak{V}_i)}{p^{Ri}}$ $(i = 1, \ldots, n)$ und $\varepsilon_0 = \dfrac{e_0 p^{R_1} - \chi(\mathfrak{V}_0)}{e_0 p^{R_1}}$ gleich 0 oder 1 sind, und zwar so, daß wenn einer gleich 0 ist, auch alle folgenden gleich 0 sind. Aus dieser Schreibweise sieht man sofort, daß die einzelnen Summanden des Exponenten ganze Zahlen sind. Die Formel (5) kann aus der gemäß Satz 2 für Exp. $\mathfrak{f}_\mathfrak{p}(K/k)$ gebildeten dadurch gewonnen werden, daß man an die einzelnen Glieder die Korrekturfaktoren ε_i anbringt, die gleich 0 zu setzen sind, sobald $K(\chi)$ im entsprechenden Verzweigungskörper K_{i-1} enthalten ist.

12. Bildet man in (5) die Summe über alle Charaktere χ und vergleicht mit der bekannten Formel für die $\mathfrak{p}$-Diskriminante:

$$\text{Exp. } \mathfrak{d}_\mathfrak{p}(K/k) = gf(e_0 p^{R_1} - 1 + v_1(p^{R_1} - 1) + (v_2 - v_1)(p^{R_2} - 1) + \cdots),$$

wo g, f die übliche Bedeutung für das Primideal $\mathfrak{p}$ haben [14]), so ergibt sich endlich die Produktformel:

$$\prod_\chi \mathfrak{f}_\chi = \mathfrak{d}.$$

Man hat dabei zu beachten, daß $\sum_\chi \chi(\mathfrak{V}_0) = e_0 p^{R_1} gf$ und allgemein $\sum_\chi \chi(\mathfrak{V}_i) = p^{Ri} e_0 gf$ ist.

13. Eine Anwendung. Wir geben jetzt noch eine Anwendung der gefundenen Formel für den $\mathfrak{p}$-Führer auf das Hassesche Normenrestsymbol $\left(\dfrac{\beta, K}{\mathfrak{p}}\right)$.

Es ist bekannt, daß dieses für alle Zahlen $\beta \neq 0$ des Grundkörpers k erklärte Symbol dann und nur dann gleich 1 ist, wenn β Normenrest mod. $\mathfrak{f}_\mathfrak{p}(K/k)$ von K ist [15]). Diesem Satz kann man einen ihm gleichwertigen zur Seite stellen, der uns Auskunft über den Wertevorrat des Symbols gibt, der entsteht, wenn (bei festem $\mathfrak{p}$) β die Zahlen bestimmter Zahlgruppen aus dem Grundkörper k durchläuft.

Dieser Satz lautet:

Satz 4. *Es sei K^* ein Teilkörper von K der den Zerlegungskörper $K_\mathfrak{z}$ zu $\mathfrak{p}$ enthält. Durchläuft dann β die Gruppe der Normenreste* mod. $\mathfrak{f}_\mathfrak{p}(K^*/k)$ *von K^*, so ist der Wertevorrat des Symbols $\left(\dfrac{\beta, K}{\mathfrak{p}}\right)$ die K^* zugeordnete Untergruppe $\mathfrak{G}^*$ von $\mathfrak{G}$.*

Beweis. Wir stützen uns auf die Übergangseigenschaft

$$\text{(6.)} \qquad \left(\frac{\beta, K}{\mathfrak{p}}\right) \to \left(\frac{\beta, K^*}{\mathfrak{p}}\right),$$

wo $\left(\dfrac{\beta, K^*}{\mathfrak{p}}\right)$ denjenigen Automorphismus von K^* bedeutet, in den $\left(\dfrac{\beta, K}{\mathfrak{p}}\right)$ bei Anwendung auf K^* übergeht (Element der Faktorgruppe $\mathfrak{G}/\mathfrak{G}^*$).

---

[13]) E. Artin, Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper, Journ. f. Math. **164** (1930).

[14]) Hasse, Bericht I a, § 8.

[15]) Hasse, Bericht II, § 7.

Daß $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ in $\mathfrak{G}^*$ liegt, ist hiernach gleichbedeutend damit, daß $\left(\frac{\beta, K^*}{\mathfrak{p}}\right) = 1$ ist, und dies weiter nach dem genannten Hasseschen Satz damit, daß β Normenrest mod. $\mathfrak{f}_\mathfrak{p}(K^*/k)$ von K^* ist. Da der gesamte Wertevorrat von $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ die Zerlegungsgruppe $\mathfrak{G}_Z$ zu $\mathfrak{p}$ ist, so entspricht also den Normenresten mod. $\mathfrak{f}_\mathfrak{p}(K^*/k)$ von K genau der Durchschnitt von $\mathfrak{G}^*$ mit $\mathfrak{G}_Z$ als Wertevorrat. Weil aber nach Voraussetzung $\mathfrak{G}^*$ in $\mathfrak{G}_Z$ enthalten ist, ist der fragliche Wertevorrat somit $\mathfrak{G}^*$ selbst, wie behauptet.

Satz 4 in Verbindung mit Satz 2 liefert uns sofort:

Satz 5. *Durchläuft β die Gruppe der Normenreste mod. $\mathfrak{p}^{1+a_\nu}$ von K_ν, so ist der Wertevorrat des Symbols $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ die ν-mal überstrichene Verzweigungsgruppe zu $\mathfrak{p}$.*

Für die Trägheitsgruppe zu $\mathfrak{p}$ hat man analog, wegen $\mathfrak{f}_\mathfrak{p}(K_T/k) = \mathfrak{p}^0$, alle Normenreste mod. $\mathfrak{p}^0$ von K_T zu betrachten. Es sind das die β_0, welche entweder zu $\mathfrak{p}$ prim sind, oder $\mathfrak{p}$ genau mit durch f teilbarem Exponenten enthalten, wo f (siehe § 12) der Relativgrad der Primteiler von $\mathfrak{p}$ in K ist [16]). Es genügt übrigens, wie eine leichte Überlegung zeigt, nur die zu $\mathfrak{p}$ primen β_0 zu berücksichtigen [17]).

---

[16]) Hasse, Bericht II, § 7, VII.

[17]) Wie ich erfahre, hat kürzlich Herr Iyanaga in diesem Zusammenhang bewiesen, daß es entsprechend für den ν-mal überstrichenen Verzweigungskörper K_ν genügt, nur die $\beta \equiv 1$ mod. $\mathfrak{p}^{1+a_\nu}$ zu berücksichtigen, und daß auch umgekehrt für jedes beliebige a der Gruppe $\beta \equiv 1$ mod. $\mathfrak{p}^{1+a}$ als Wertevorrat von $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ die einem gewissen Verzweigungskörper K_ν zugeordnete Gruppe $\mathfrak{B}_\nu$ entspricht; ν bestimmt sich dabei durch $a_\nu \leqq a < a_{\nu+1}$.

Eingegangen 22. März 1932.

La théorie du symbole de restes normiques.

Par *Claude Chevalley* à Paris.

Introduction.

M. Hasse a montré que la théorie des restes normiques modulo les puissances d'un idéal premier p dans un corps de nombres algébriques était équivalente à la théorie arithmétique des extensions des corps de nombres p-adiques [1]). Il a introduit la théorie du corps de classes local (Klassenkörpertheorie im Kleinen), dont il a, avec M. Schmidt, déduit les théorèmes de ceux de la théorie du corps de classes ordinaire (im Großen).

Mais, étant donné que la théorie du corps de classes local est plus simple que la théorie générale, il y avait interêt à baser cette théorie d'une manière indépendante. C'est ce qui a été fait simultanèment par M. Schmidt et par l'auteur [2]), qui démontrent d'une manière purement arithmétique, par des voies d'ailleurs différentes, les théorèmes de la théorie du corps de classes local. Ces théorèmes s'énoncent ainsi: étant donné un corps de nombres p-adiques k dans lequel le groupe des nombres $\neq 0$ sera désigné par k^* on appelle *groupe associé* dans k à un sur-corps K le groupe des nombres $\neq 0$ de k qui sont normes relatives par rapport à k de nombres de K; ceci posé:

1. Si K est un sur-corps relativement abélien de k de degré relatif n, le groupe H associé à K dans k est un sous-groupe d'indice n de k^*. On exprime ce fait en disant que K est corps de classes sur k pour le groupe H.

2. En se plaçant dans les hypothèses de 1, le groupe k^*/H est isomorphe au groupe de Galois de K par rapport à k.

3. Si deux sur-corps relativement abéliens de k sont distincts, les groupes qui leur sont associés dans k sont distincts.

4. Pour tout sous-groupe de k^* d'indice fini, il existe un sur-corps relativement abélien de k qui est corps de classes sur k pour ce groupe.

Les théorèmes 1, 2, 3, 4 sont respectivement appelés *théorèmes réciproque, d'isomorphie, d'unicité, d'existence.*

M. Hasse avait montré que le symbole de restes normiques fournit une réalisation de l'isomorphisme affirmé par le théorème 2. Mais on n'avait pas encore réussi à fonder la théorie de ce symbole d'une manière indépendante de la théorie du corps de classes ordinaire. C'est cette lacune qu'on se propose de combler ici.

---

[1]) Voir H. 1 et Schmidt 1.

[2]) Les démonstrations de M. Schmidt ne sont pas publiées. On trouvera les miennes dans ma thèse, à paraitre prochainement sous le titre „La théorie du corps de classes".

Nous donnons du symbole de restes normiques une définition fondée sur la théorie des systèmes de nombres hypercomplexes, et nous montrons que le symbole ainsi obtenu satisfait aux règles de calcul bien connues du symbole de restes normiques. Cette définition coïncide, à la façon de parler près, avec celle de M. Hasse dans H. 5, dans le cas des extensions cycliques, ces définitions ayant d'ailleurs été trouvées indépendamment l'une de l'autre. Au surplus, l'idée de la définition en question m'a été donnée par une remarque de Mlle. Noether dans ses leçons dactylographiées sur la théorie des algèbres.

Les règles de calcul ne définissent pas entièrement le symbole de restes normiques: elles subsistent par exemple si on remplace chaque symbole par son inverse. La coïncidence de notre symbole avec le symbole précédemment défini dans un cas particulier démontre leur identité.

Notations.

Dans le cours de ce travail, k désignera toujours (sauf au § 9) un corps local (c'est-à-dire un corps de nombres p-adiques); k^* sera le groupe des nombres $\neq 0$ de k; p sera un nombre de k représentant l'idéal premier de ce corps; nous introduirons divers autres corps $K, Z, \ldots$ qui seront aussi des corps locaux. Pour chacun de ces corps, on désignera par la lettre p affectée en indice de la lettre qui représente le corps un nombre représentant l'idéal premier du corps.

Si un sous-groupe H de k^* est à groupe quotient cyclique, on appellera *primitif* par rapport à H un nombre β de k qui est tel que la classe de β mod. H engendre le groupe quotient k^*/H.

Si K est un sur-corps relativement galoisien, dont le groupe de Galois est composé des opérations $1, s, t, \ldots$, et si $a_{s,t}$ constitue un système de facteurs de K, l'algèbre produit intérieur (verschränktes Produkt) de K par son groupe avec le système de facteurs $a_{s,t}$ sera désignée par (a, K).

Si K est relativement cyclique par rapport à k, soit s une opération engendrant son groupe de Galois, et soit β un nombre $\neq 0$ de k. L'algèbre sur k déduite de l'adjonction à K d'un élément u tel que $u^n = \beta$ [où $n = (K : k)$] et que, pour tout élément x de K, $xu = ux^s$, sera désignée par (β, K, s). Si il y a lieu de préciser le centre de cette algèbre, on écrira $(\beta, K, s)_k$.

Les algèbres A, A' ayant même centre, on sait qu'on dit qu'elles sont semblables, quand elles sont algèbres complètes de matrices sur un même corps gauche. On désignera cette relation par la notation $A \sim A'$.

Si A est une algèbre de centre k, et si K est une extension de k, on désignera par A_K l'algèbre de centre K obtenue comme produit direct de A et de K.

Références.

A. A. Albert, 1. Normal division algebras. Trans. of the Amer. Math. Soc. **34** (1932).

R. Brauer, 1. Über die algebraische Struktur von Schiefkörpern. Journ. für Math. **166** (1932).

M. Deuring, 1. Zur Theorie der Normen relativzyklischer Körper. Göttinger Nachrichten 1931.

H. Hasse, H. 1. Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen. Journ. für Math. **162** (1930).

—, H. 2. Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme. Math. Ann. **104** (1931).

—, H. 3. Theory of cyclic algebras over an algebraic number field. Trans. of the Amer. Math. Soc. **34** (1932).

H. Hasse, H. 4. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Leipzig 1930.

—, H. 5. Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. Math. Ann. **107** (1933).

—, H. 6. (Avec R. Brauer et E. Noether.) Beweis eines Hauptsatzes in der Theorie der Algebren. Journ. für Math. **167** (1932).

G. Köthe, 1. Erweiterung des Zentrums einfacher Algebren. Math. Ann. **107** (1933).

F. K. Schmidt, 1. Zur Klassenkörpertheorie im Kleinen. Journ. für Math. **162** (1930).

B. v. d. Waerden, 1. Moderne Algebra II. Berlin 1931.

I. La théorie du corps de classes relativement cyclique.

La particularité la plus remarquable des algèbres dont le centre est un corps de nombres p-adiques k est de contenir tous les sur-corps de k de degré relatif égal au degré de l'algèbre. Nous donnons ici de ce théorème la démonstration de M. Hasse (voir H. 6, Th. 3), et nous en tirons, comme le fait M. Hasse dans H. 5, la conséquence que les sur-corps relativement cycliques d'un corps k sont corps de classes par rapport à k. Mlle. Noether avait d'ailleurs depuis longtemps remarqué le lien entre la théorie développée dans H. 2 et la théorie des corps de classes locaux.

Théorème 0. *Soit A une algèbre simple de centre k, de degré n. Soit K une extension de degré n de k. A contient un corps isomorphe à K.*

En effet, A est une algèbre complète de matrices à coefficients dans un corps gauche de centre k, de degré n'. Soit W le sur-corps relativement cyclique non ramifié de k de degré n' [3]). Il résulte de H. 2, Th. 38 que A est semblable à une algèbre de la forme (p, W, s), s étant un automorphisme engendrant le groupe de W par rapport à k. On a (H. 3, 15. 5)

$$A_K \sim (p, W^K, s_K),$$

où s_K est la plus petite puissance de s qui produise un automorphisme du corps composé W^K de W et de K par rapport à K. Soient φ, ε le degré et l'exposant relatifs de (p_K) par rapport à k. On a $\varphi\varepsilon = n$, et W^K est le sur-corps relativement cyclique non ramifié de K de degré $\frac{n'}{(n', \varphi)}$. On a $(p) = (p_K)^\varepsilon$, et ε est multiple de $\frac{n'}{(n', \varphi)}$. Par suite, p, considéré comme nombre de K, est norme relative d'un nombre de W^K, et par suite $A_K \sim 1$. Donc K est un corps de décomposition de A, et par suite est isomorphe à un sous-corps commutatif maximum d'une algèbre de degré n isomorphe à A. A étant de degré n, cette algèbre est A elle-même.

Supposant K cyclique par rapport à k, soit σ une opération engendrant son groupe relatif de Galois: il résulte du Th. 0 que toute algèbre simple A de centre k et de degré n se met sous la forme (β, K, σ), β étant un nombre $\neq 0$ de k. La correspondance $\beta \to A$ est une homomorphie de k^* et du groupe des classes d'algèbres de centre k contenant des algèbres de degré n. Dans cette homomorphie, on sait que les éléments du groupe H associé à K dans k et ceux-la seuls, donnent la classe unité. Donc:

Si H est le groupe associé au corps relativement cyclique K dans k, le groupe k^*/H est isomorphe au groupe des classes d'algèbres simples de centre k contenant des algèbres de degré n.

---

[3]) Voir H. 2, Th. 25, 26, 27.

Supposant en particulier que K soit non ramifié, il resulte de H. 2, Th. 27 que k^*/H est un groupe cyclique de degré n. Par suite la même propriété est vraie pour toutes les extensions relativement cycliques, *ce qui démontre le théorème réciproque et le théorème d'isomorphie pour les extensions cycliques.*

II. Lemmes sur les algèbres de centre k.

Lemme 1. *Soit K un sur-corps relativement cyclique de degré n de k, dont le groupe de Galois est engendré par une opération s. β étant un nombre $\neq 0$ de k, soit $A = (\beta, K, s)$. d étant un diviseur de n, soit K' le sous-corps de K de degré $\frac{n}{d}$ par rapport à k. On a $A^d \sim (\beta, K', s)$* [4]).

On peut sans restriction supposer dans la démonstration que A est un corps gauche, c'est-à-dire que le nombre β soit un nombre primitif pour le groupe H associé à K dans k, car tout nombre β est congru à une puissance d'un nombre primitif modulo H, et a fortiori modulo le groupe associé à K'. Nous considérerons de plus K comme contenu dans A.

Remarquons que A^d appartient à une classe d'algèbres d'exposant $\frac{n}{d}$. Donc cette algèbre est algèbre complète de matrices sur un corps gauche d'exposant $\frac{n}{d}$, de centre k, donc aussi de degré $\frac{n}{d}$. D'autre part $A^d \sim (\beta^d, K, s)$. Le second membre est une algèbre de degré n, qui, d'après ce que nous venons de dire est somme directe d'idéaux à droite minima, dont chacun est par suite k-module de rang $\frac{n^2}{d}$. De plus le corps gauche sur lequel A^d est algèbre complète de matrices est inversement isomorphe au corps des opérateur-isomorphismes d'un de ces idéaux à droite minima. Soit $A' = (\beta^d, K, s)$. A' contient un élément u tel que $u^n = \beta^d$ et que, pour tout élément x de K on ait $xu = ux^s$. Considérons le sous-anneau $\mathfrak{o}$ de A' engendré par les nombres de K' et par u. C'est une algèbre dont le centre est l'anneau engendré par les nombres de k et par $u^{\frac{n}{d}}$. Soit v ce dernier élément. On a $v^d = \beta^d$, et on sait que l'algèbre commutative (k, v) est somme directe des corps définis par les facteurs irreductibles de $x^d - \beta^d$ dans k [5]). L'un de ces facteurs est $x - \beta$, et par suite il existe dans cette algèbre un idempotent e tel que $v\,e = \beta\,e$. On a $\mathfrak{o}\,e = (K'e, u\,e)$ et ue satisfait aux conditions suivantes: $(u\,e)^{\frac{n}{d}} = \beta\,e$, $x(u\,e) = (u\,e)x^s$ pour tout nombre x de $K'e$. Donc $\mathfrak{o}\,e = (\beta, K', s)$. β étant primitif pour le groupe associé à K' dans k, (β, K', s) est un corps gauche. Considérons eA': cet ensemble résulte de l'adjonction à $\mathfrak{o}\,e = e\,\mathfrak{o}$ des nombres de eK. eK' étant contenu dans eK, et $e\mathfrak{o}$ étant k-module de rang $\left(\frac{n}{d}\right)^2$, eA' est k-module de rang $\leqq \frac{n^2}{d}$. Mais c'est d'autre part un idéal à droite de A'. C'est donc un idéal à droite minimum. Les éléments de (β, K', s) qui

---

[4]) Ce théorème a été démontré par A. A. Albert et par H. Hasse pour des corps de bases généraux. Voir H. 5.

[5]) En effet, (k, v) est l'anneau des restes de l'ensemble des polynomes à coefficients dans k modulo l'idéal $(x^d - \beta^d)$. Si Ke est l'un des éléments de cette somme de corps, e étant idempotent, xe satisfait à l'équation obtenue en annulant le facteur irreductible correspondant de $x^d - \beta^d$.

est un corps gauche contenu dans eA' fournissent des opérateur-isomorphismes de cet idéal, et comme (β, K', s) est de rang $\left(\frac{n}{d}\right)^2$, ils les fournissent tous, ce qui montre que le corps gauche sur lequel A' est algèbre complète de matrices est isomorphe à (β, K', s).

Lemme 2. *Soient K un sur-corps de k de degré relatif n, et A une algèbre de centre k contenant un sous-corps $\bar{K}$ isomorphe à K. Soit A' l'algèbre des éléments de A permutables à tous les éléments de $\bar{K}$. On a $A' \sim A_K$* [5a]).

En effet, $\bar{K}$ est contenu dans un sous-corps commutatif maximum $\bar{K}^*$ de A. En remplaçant au besoin A par une algèbre semblable, on peut supposer $\bar{K}^*$ galoisien par rapport à k. (On ne fait en remplaçant A par une algèbre semblable que remplacer A_K et A' par des algèbres semblables.) Donc A est produit intérieur de $\bar{K}^*$ par son groupe avec un système de facteurs $a_{s,t}$. Soient $u_s, u_t, \ldots$ les nombres de A produisant par transformation [6]) les divers automorphismes $s, t, \ldots$ L'algèbre A' est composée des expressions linéaires $\Sigma x_s u_s$ à coefficients dans $\bar{K}^*$ qui ne contiennent que les u_s relatifs aux opérations du groupe de $\bar{K}^*$ par rapport à $\bar{K}$. Par suite $A' = (a^K, \bar{K}^*)$, a^K désignant les éléments du système de facteurs (a) relatifs aux opérations du groupe de $\bar{K}^*$ par rapport à $\bar{K}$. Mais ce produit intérieur est précisément isomorphe à A_K en vertu de H. 3, 14.

On remarquera que ce lemme est valable pour tous les corps de base pour lesquels est valable la théorie des produits intérieurs.

Nous allons avoir besoin dans la théorie des restes normiques d'isoler dans le système des corps gauches de degré n de centre k un corps gauche particulier. C'est pourquoi nous posons la définition suivante:

Soit W le sur-corps relativement cyclique non ramifié de k de degré n. Soit s l'inverse de la substitution de Frobenius $\left(\frac{W}{(p)}\right)$ [7]). Nous appellerons *corps gauche normé* de centre k de degré n l'algèbre (p, W, s) [8]).

Il résulte alors immédiatement du lemme 1 le

Lemme 3. *Si $\mathfrak{K}$ est le corps gauche normé de centre k de degré n, et si d est diviseur de n, $\mathfrak{K}^d$ est semblable au corps gauche normé de centre k de degré $\frac{n}{d}$.*

Au lemme 2 correspond de même le

Lemme 4. *Si $\mathfrak{K}$ est un corps gauche normé de centre k, et si K est une extension de k contenue dans $\mathfrak{K}$, l'ensemble $\mathfrak{K}'$ des éléments de $\mathfrak{K}$ permutables à tous les éléments de K est un corps gauche normé de centre K* [9]).

En effet, les notations étant les mêmes que dans la définition du corps gauche normé, on a (lemme 2) $\mathfrak{K}' \sim \mathfrak{K}_K$. Mais, en vertu de H. 3, 15. 5, on a $\mathfrak{K}_K \sim (p, W^K, s_K)$, où

[5a]) Pour ce lemme, voir déjà v. d. Waerden, 1, § 128. Récemment il a été démontré aussi par R. Brauer, 1.

[6]) Nous entendons par là que pour tout élément x de $\bar{K}^*$, on a $u_s^{-1} x u_s = x^s$.

[7]) Rappelons que la substitution de Frobenius est l'automorphisme de W qui change tout entier A en un entier $\equiv A^{N(p)}$ (mod. (p)). Voir pour les propriétés de ce symbole H. 4, II, § 1.

[8]) Dans la terminologie de M. Hasse, le corps gauche normé de degré n définit la classe d'algèbres d'invariant $\frac{1}{n}$.

[9]) En tenant compte de la note (8), ce théorème est équivalent à un théorème de M. Köthe. Voir Köthe, 1.

W^K est le corps composé de W et de K, et où s_K est la plus petite puissance de s qui produise un automorphisme de W^K par rapport à K. Or s_K est l'inverse de la substitution de Frobenius $\left(\frac{W^K/K}{(p_K)}\right)$; en effet on sait que

$$\left(\frac{W^K/K}{(p_K)}\right) = \left(\frac{W}{N_{Kk}\mathfrak{p}_K}\right) = \left(\frac{W}{(p^\varphi)}\right),$$

où φ est le degré relatif de (p_K) par rapport à k. φ est encore égal au degré de $[W, K]$ par rapport à k, donc encore à $(W^K : K)$, et par suite $s_K = s^\varphi$. D'autre part si ε est l'exposant relatif de l'idéal premier (p_K) par rapport à k, l'algèbre (p, W^K, s_K) est semblable à $(p_K, W^K, s_K)^\varepsilon$. L'algèbre (p_K, W^K, s_K) est le corps gauche normé de centre K de degré $\frac{n}{\varphi}$, où φ est le degré relatif de (p_K) par rapport à k. De $\varepsilon\varphi = (K : k)$ on déduit que ε divise $\frac{n}{\varphi}$, et par suite en vertu du lemme 3, $\mathfrak{R}_K$ est semblable au corps gauche normé de centre K de degré $\frac{n}{\varphi\varepsilon} = \frac{n}{(K : k)}$. Deux corps gauches semblables étant isomorphes, le lemme 4 est démontré.

III. Définition du symbole de restes normiques pour les extensions cycliques [10]).

Soit K un sur-corps relativement cyclique de k de degré relatif n, corps de classes sur k pour le groupe H. Soient s une opération engendrant le groupe de Galois de K par rapport à k, β un nombre $\neq 0$ de k et $\mathfrak{R}$ le corps gauche normé de centre k de degré n. La classe de ce corps gauche engendre le groupe des classes d'algèbres simples de centre k qui contiennent des algèbres de degré n. Par suite, il existe un exposant a determiné mod. n tel que

$$(\beta, K, s) \sim \mathfrak{R}^a.$$

Nous appellerons *symbole de restes normiques* de β par rapport à K et nous désignerons par $\left(\frac{\beta, K}{p}\right)$ [ou, s'il y a lieu d'indiquer explicitement le corps de base, par $\left(\frac{\beta, K/k}{p}\right)$] la substitution s^a. Il faut d'abord montrer que cette définition est indépendante de la substitution s choisie pour engendrer le groupe de Galois de K. Soit en effet $s' = s^r$, $(r, n) = 1$, une autre substitution primitive. L'algèbre (β, K, s) contient un élément u tel que la transformation par u produise sur les nombres de K l'automorphisme s et que $u^n = \beta$. Posons $u^r = v$: on a $v^n = \beta^r$, et la transformation par v produit l'automorphisme s'. On a donc

$$(\beta, K, s) = (\beta^r, K, s') \sim (\beta, K, s')^r.$$

Si donc $(\beta, K, s') \sim \mathfrak{R}^{a'}$, on a $a'r \equiv a \pmod{n}$ d'où $s'^{a'} = s^a$ ce qui démontre notre proposition.

Théorème 1. *La condition necessaire et suffisante pour que β soit norme par rapport à k d'un nombre de K est que* $\left(\frac{\beta, K}{p}\right) = 1$.

---

10) La définition du symbole de restes normiques donnée dans ce paragraphe coïncide, comme nous l'avons dit dans l'introduction, avec celle donnée par M. Hasse dans H. 5. On trouvera également dans ce mémoire des démonstrations des théorèmes 1, 2, 3.

En effet, la condition necessaire et suffisante pour que β soit norme relative d'un nombre de K est que $(\beta, K, s) \sim 1$, c'est-à-dire, en reprenant les notations de la définition, que $a \equiv 0 \pmod{n}$, ce qui démontre le théorème.

Théorème 2. *β, β' étant deux nombres $\neq 0$ de k, on a*

$$\left(\frac{\beta\beta', K}{p}\right) = \left(\frac{\beta, K}{p}\right)\left(\frac{\beta', K}{p}\right).$$

Cela résulte immédiatement de la formule

$$(\beta\beta', K, s) \sim (\beta, K, s)\,(\beta', K, s).$$

Théorème 3. *Si K' est un sous-corps de K, on a*

$$\left(\frac{\beta, K}{p}\right) \to \left(\frac{\beta, K'}{p}\right),$$

la fléche indiquant que l'automorphisme du second membre est l'automorphisme de K' induit par l'automorphisme du premier membre.

En effet, soit $d = (K : K')$. Il résulte du lemme 1 que

$$(\beta, K, s)^d \sim (\beta, K', s).$$

Soit $\left(\frac{\beta, K}{p}\right) = s^a$, et par suite $(\beta, K, s) \sim \mathfrak{R}^a$ et $(\beta, K', s) \sim \mathfrak{R}^{ad}$. Mais, en vertu du lemme 3, $\mathfrak{R}^d$ est semblable au corps gauche normé de centre k de degré $\frac{n}{d}$, ce qui démontre le théorème.

Théorème 4. *Si K' est un sous-corps de K, et si B est un nombre $\neq 0$ de K', on a*

$$\left(\frac{B, K/K'}{p_{K'}}\right) = \left(\frac{N_{K'k}(B), K}{p}\right)^{11}).$$

(Le groupe de Galois de K/K' est identifié à un sous-groupe du groupe de Galois de K/k.)

Supposons d'abord que B soit un nombre β_0 de k primitif pour le groupe H associé à K dans k. Soit $s = \left(\frac{\beta_0, K}{p}\right)$. s est une opération primitive du groupe de K/k. La plus petite puissance de s laissant invariants les nombres de K' est $s^{\frac{n}{d}}$, si $d = (K : K')$, et par suite (lemme 2) l'algèbre des éléments de (β_0, K, s) permutables avec les éléments de K' est $(\beta_0, K, s^{\frac{n}{d}})_{K'}$. D'autre part, (β_0, K, s) est le corps gauche normé de centre k de degré n. Donc (lemme 4) $(\beta_0, K, s^{\frac{n}{d}})_{K'}$ est le corps gauche normé de centre K' de degré d, ce qui démontre le théorème dans ce cas particulier:

en effet
$$\left(\frac{\beta_0, K/K'}{p_{K'}}\right) = s^{\frac{n}{d}} = \left(\frac{\beta_0^{\frac{n}{d}}, K}{p}\right) = \left(\frac{N_{K'k}(\beta_0), K}{p}\right).$$

Il en résulte en particulier que β_0 est dans K' un nombre primitif pour le groupe associé à K dans K'. Par suite, si B est un nombre quelconque différent de 0 de K', on a $B = \beta_0^a N_{KK'}(\Gamma)$, Γ étant un nombre de K. D'où

---

11) On trouvera une démonstration d'un théorème à peu près équivalent au précédent dans Köthe 1.

$$\left(\frac{B,\ K/K'}{p_{K'}}\right)=\left(\frac{\beta_0^a,\ K/K'}{p_{K'}}\right)=\left(\frac{\beta_0^{a\frac{n}{d}},\ K}{p}\right)=\left(\frac{N_{K'k}(B)\,N_{Kk}(\Gamma^{-1}),\ K}{p}\right)=\left(\frac{N_{K'k}(B),\ K}{p}\right),$$

ce qui démontre le théorème dans le cas général.

IV. Demonstration d'un lemme sur les systèmes de facteurs.

Dans ce paragraphe, k désignera un corps de base parfait quelconque, et Z une extension galoisienne de k composée de deux extensions Z_1, Z_2 galoisiennes par rapport à k et étrangères l'une à l'autre (fremd), de sorte que le groupe de Galois G de Z par rapport à k est produit direct des groupes de Galois g, g' de Z par rapport à Z_1, Z_2. Les opérations de g seront désignées par $1, s, s', \ldots$ et celles de g' par $1, t, t', \ldots$ Considérons un système de facteurs (a) de Z et l'algèbre A qui lui correspond. Soit n l'ordre de g. Nous nous proposons de démontrer le lemme suivant:

Lemme 5. *L'algèbre A^n est semblable à l'algèbre (a', Z_1), le système de facteurs (a') du corps Z_1 étant défini par*

$$a'_{t,t'} = N_{ZZ_1}(a_{t,t'})\ ^{12}).$$

En effet, soient $u_s, u_t, \ldots$ des éléments de A qui produisent sur les nombres de Z les automorphismes $s, t, \ldots$, et dont les règles de multiplication sont données par les éléments du système de facteurs (a). On peut toujours, sans changer les $a_{t,t'}$ supposer que $a_{s,t} = 1$ pour tout couple s, t [13]).

Nous allons d'abord former d'autres systèmes de facteurs équivalents au système (a) [14]). Pour cela, considérons une opération fixe s du groupe g, et posons

$$\bar{u}_{s'} = u_{s'} \quad \bar{u}_t = u_s^{-1} u_t u_s = u_t a_{t,s} \quad \bar{u}_{s't} = \bar{u}_{s'}\bar{u}_t.$$

Ces éléments produisent les automorphismes qui leur sont affectés en indices. Calculons les systèmes de facteurs $(\bar{a})$ relatif à ces nouvelles unités. On a

$$u_s^{-1} u_t u_s \cdot u_s^{-1} u_{t'} u_s = u_s^{-1} u_{tt'} u_s \cdot a_{t,t'}^s$$

et

$$u_s^{-1} u_t u_s \cdot u_{s'} = u_{s'} \cdot u_s^{-1} u_t u_s \cdot \bar{a}_{t,s'},$$

d'où

$$a_{s,s'}^{-1} u_{ss'}^{-1} u_t u_{ss'} a_{s,s'} = u_t a_{t,s} \bar{a}_{t,s'},$$

d'où on tire facilement

$$\bar{a}_{s,s'} = a_{s,s'}; \quad \bar{a}_{t,t'} = a_{t,t'}^s; \quad \bar{a}_{t,s'} = a_{s,s'}^{1-t} a_{t,ss'} \ a_{t,s}^{-1}$$

et naturellement $\bar{a}_{s,t} = 1$. Faisons le produit des systèmes de facteurs ainsi obtenus pour les différents s. On obtiendra un système de facteurs de Z définissant A^n. Ce système de facteurs est donné par les formules:

$$\bar{\bar{a}}_{s,s'} = a_{s,s'}^n; \quad \bar{\bar{a}}_{t,t'} = N_{ZZ_1}(a_{t,t'}); \quad \bar{\bar{a}}_{t,s'} = d_{s'}^{1-t}$$

---

12) Ce lemme a été démontré dans le cas particulier où g, g' sont des groupes cycliques d'ordres premiers par A. A. Albert, 1.

13) En effet, supposons $a_{s,t} \neq 1$, $u_s u_t = u_{st} \cdot a_{s,t}$. Comme toute opération de G peut se mettre d'une manière et d'une seule sous la forme st, on peut faire le changement d'unités défini par les formules $u'_s = u_s$, $u'_t = u_t$, $u'_{st} = u_{st}\ a_{s,t} = u'_s u'_t$.

14) Nous appelons deux systèmes de facteurs pour un même corps équivalents quand ils définissent des algèbres isomorphes.

avec bien entendu $\bar{\bar{a}}_{s,t} = 1$. On a posé

$$d_{s'} = \Pi_s a_{s,s'} .$$

D'autre part les relations d'associativité des systèmes de facteurs s'écrivent

$$a_{ss',s''} \cdot a_{s,s'}^{s''} = a_{s',s''} \cdot a_{s,s's''},$$

et en multipliant entre elles les formules relatives aux différents s, il vient

$$a_{s',s''}^{n} = \frac{d_{s''} d_{s'}^{s''}}{d_{s's''}}.$$

Ceci posé, l'algèbre $(\bar{a}, Z)$ contient des éléments $\bar{\bar{u}}_{st}$ produisant par transformation les divers automorphismes st, et dont les règles de multiplication sont données par le système de facteurs $\bar{a}$. Posons

$$u'_s = \bar{\bar{u}}_s d_s^{-1}, \; u'_t = \bar{\bar{u}}_t, \; u'_{st} = u'_s u'_t .$$

Ces nouvelles unités définissent un système de facteurs (a') qui se calcule facilement: il vient

$$a'_{s,s'} = 1; \; a'_{t,t'} = N_{ZZ_1}(a_{t,t'}); \; a'_{s,t} = a'_{t,s} = 1.$$

Les deux derniéres formules montrent que les u'_s sont permutables avec les u'_t, et par suite l'algèbre A^n est semblable au produit direct de l'algèbre $(a'_{s,s'}, Z_2)$ qui est une algèbre complète de matrices à coefficients dans k, et de l'algèbre $(a'_{t,t'}, Z_1)$; ce qui démontre le lemme.

V. Le symbole de restes normiques pour des extensions abéliennes quelconques.

Le lemme du paragraphe IV va nous permettre de démontrer le „théorème de translation" du symbole de restes normiques, qui s'énonce de la manière suivante:

k étant corps de nombres p-adiques, soient K un sur-corps relativement cyclique de k et Z une extension galoisienne de k. Alors:

Théorème 5. *B étant un nombre quelconque $\neq 0$ de Z, on a*

$$\left(\frac{B, KZ/Z}{pz}\right) = \left(\frac{N_{Zk}(B), K}{p}\right).$$

(Le groupe de Galois de KZ par rapport à Z est identifié à un sous-groupe du groupe de Galois de K par rapport à k.)

Nous supposerons d'abord K et Z étrangers par rapport à k, de sorte que le groupe de Galois de KZ par rapport à k soit le produit direct des groupes de Galois de K et de Z. Nous supposerons également, ce qui n'est evidemment pas une restriction, que le nombre B est primitif par rapport au groupe de nombres de Z associé à KZ. Considérons le corps gauche normé $\mathfrak{R}$ de centre k de degré égal à celui de KZ. L'algèbre des éléments de ce corps permutables avec tous les éléments de Z est le corps gauche de centre Z de degré $m = (KZ : Z) = (K : k)$ (lemme 4), et par suite ce corps gauche est l'algèbre (B, KZ, s) où on a posé $s = \left(\frac{B, KZ/Z}{pz}\right)$. D'autre part $\mathfrak{R}$ se laisse représenter comme produit intérieur de KZ par son groupe, et on peut supposer que si u_s est l'élément qui produit par transformation l'automorphisme s de KZ, on a $u_{si} = (u_s)^i$ $(i = 0, 1, \ldots, m-1)$ et $u_s^m = B$. En effet $(u_s)^m$ est certainement un élément permutable avec tous les éléments de KZ, et de plus permutable avec u_s, donc un élément de Z; de plus l'algèbre (B, KZ, s) des éléments de $\mathfrak{R}$ permutables avec tous les éléments de Z est engendrée par KZ et par u_s,

et par suite $(u_s)^m$ ne diffère de B que par multiplication par la norme relative par rapport à Z d'un nombre de KZ.

Appliquons le lemme du paragraphe précédent. Si $n = (Z : k)$, il résulte tout de suite de ce lemme que $\mathfrak{R}^n \sim (N_{Zk}(B),\ K, s)$. Mais, en vertu du lemme 3, $\mathfrak{R}^n$ est semblable au corps gauche normé de centre k de degré m, et par suite

$$\left(\frac{N_{Zk}(B),\ K}{p}\right) = s,$$

ce qui démontre le théorème dans le cas particulier considéré.

Passons maintenant au cas général, et soit $[K, Z] = k'$. Alors, en vertu de la première partie de la démonstration, on a

$$\left(\frac{N_{Zk'}(B),\ K/k'}{p_{k'}}\right) = \left(\frac{B,\ KZ}{pz}\right).$$

Mais, en vertu du théorème 4, on a

$$\left(\frac{N_{Zk}(B),\ K}{p}\right) = \left(\frac{N_{Zk'}(B),\ K/k'}{p_{k'}}\right),$$

ce qui démontre le théorème 5.

Ceci posé considérons un sur-corps relativement abélien K de k dont le groupe de Galois G est le produit direct de h groupes cycliques g_i, engendrés par des opérations s_i. Soit K_i le sous-corps de K qui appartient au groupe composé de tous les $g_j (j \neq i)$. Les corps K_i sont des sur-corps relativement cycliques de k de degrés relatifs n_i. Ils sont corps de classes sur k pour des groupes H_i. Soit H la partie commune à tous les H_i. Soit $s = \Pi\, s_i^{a_i}$ une opération quelconque de G, et soit K_s le sous-corps de K appartenant au groupe engendré par s. Le corps K étant sur-corps relativement cyclique de K_s, nous pouvons choisir dans K_s un nombre B_s tel que

$$\left(\frac{B_s,\ K/K_s}{p_{K_s}}\right) = s.$$

Posons $N_{K_s k}(B_s) = \beta_s$. En vertu du théorème 3 on a

$$s \to \left(\frac{B_s,\ K_i K_s/K_s}{p_{K_s}}\right).$$

Le théorème 5 donne alors

$$s \to \left(\frac{\beta_s,\ K_i}{p}\right), \quad \text{c'est-à-dire} \quad \left(\frac{\beta_s,\ K_i}{p}\right) = s_i^{a_i}.$$

Par suite, il est toujours possible de trouver un nombre de k tel que les symboles de restes normiques de ce nombre dans les divers corps K_i aient des valeurs quelconques données à l'avance; ce nombre est evidemment determiné à la multiplication près par un nombre de H. Par suite le groupe H est un sous-groupe d'indice $n = \Pi n_i$ de k^*, et le groupe k^*/H est isomorphe au groupe de Galois de K par rapport à k. Montrons que H est le groupe associé à K dans k. Le groupe associé à K dans k est evidemment contenu dans tous les groupes H_i, et par suite dans H. Montrons reciproquement que tout nombre de H est norme relative par rapport à k d'un nombre de K. Soit Z_i le corps composé de $K_1, K_2, \ldots, K_i$. Un nombre β de H est norme relative d'un nombre de Z_1. Supposons démontré qu'il est norme relative d'un nombre B_i de Z_i. On a, en vertu du théorème 5,

$$\left(\frac{B_i,\ Z_{i+1}/Z_i}{pz_i}\right)=\left(\frac{B_i,\ K_{+1}\ Z_i/Z_i}{pz_i}\right)=\left(\frac{\beta,\ K_{i+1}}{p}\right)=1,$$

et par suite B_i est norme relative par rapport à Z_i d'un nombre de Z_{i+1}, donc β est norme relative par rapport à k d'un nombre de Z_{i+1}. Comme $Z_h = K$, β appartient au groupe associé à K dans k.

Nous avons démontré d'une manière générale les théoremès réciproque et d'isomorphie de la théorie du corps de classes local.

D'autre part choisissons, comme au début du paragraphe, pour chaque opération s de G un nombre β_s tel que

$$s \to \left(\frac{\beta_s,\ K_i}{p}\right).$$

Il y a un de ces nombres et un seul dans chaque classe de nombres de k^* mod. H, et par suite si β est un nombre $\neq 0$ de k il y a un nombre β_s et un seul tel que $\beta \equiv \beta_s$ (mod. H). L'opération s étant ainsi définie, nous poserons

$$s = \left(\frac{\beta,\ K}{p}\right),$$

et s sera appelé le symbole de restes normiques de β dans K. *Ce symbole est caractérisé par le fait que*

$$\left(\frac{\beta,\ K}{p}\right) \to \left(\frac{\beta,\ K_i}{p}\right), \tag{1}$$

comme on le voit tout de suite en remarquant que $\beta \equiv \beta_s$ (mod. H_i).

Théorème 6. *La condition necessaire et suffisante pour que β soit norme relative d'un nombre de K est que* $\left(\frac{\beta,\ K}{p}\right)=1$.

En effet, le seul nombre β_s contenu dans H est β_1.

Théorème 7. *Si β, β' sont deux nombres $\neq 0$ de k, on* a

$$\left(\frac{\beta\beta',\ K}{p}\right)=\left(\frac{\beta,\ K}{p}\right)\left(\frac{\beta',\ K}{p}\right).$$

Cela résulte du théorème 2 et de ce que $\left(\frac{\beta,\ K}{p}\right)$ est caractérisé par les formules (1).

Si K' est un sous-corps de K relativement cyclique par rapport à k, on a, β étant un nombre $\neq 0$ de k, si $\left(\frac{\beta,\ K}{p}\right)=s$,

$$s \to \left(\frac{B_s,\ K'\ K_s/K_s}{p_{K_s}}\right)$$

et par suite

$$s \to \left(\frac{\beta_s,\ K'}{p}\right)=\left(\frac{\beta,\ K'}{p}\right).$$

Ceci montre que la définition de notre symbole de restes normiques est indépendante du choix des corps relativement cycliques K_i dont le corps composé est K. De plus comme tout sous-corps de K est composé de corps relativement cycliques par rapport à k, on a le

Théorème 8. *Si K' est un corps compris entre K et k, on a*

$$\left(\frac{\beta, K}{p}\right) \to \left(\frac{\beta, K'}{p}\right).$$

Théorème 9. *Si Z est un sur-corps relativement galoisien de k, et si B est un nombre $\neq 0$ de Z, on a*

$$\left(\frac{B, KZ/Z}{pz}\right) = \left(\frac{N_{Zk}(B), K}{p}\right).$$

En effet, K est composé de corps relativement cycliques par rapport à k. Soient K_i ces corps. On a

$$\left(\frac{B, KZ}{pz}\right) \to \left(\frac{B, K_iZ/Z}{pz}\right) = \left(\frac{N_{Zk}(B), K_i}{p}\right),$$

d'où résulte le théorème, puisque le symbole de restes normiques d'un nombre de k par rapport à K est univoquement caractérisé, quand on connait ses symboles de restes normiques par rapport aux K_i.

D'une manière générale, si K est composé de corps relativement abéliens par rapport à k, le symbole de restes normiques d'un nombre de k est univoquement determiné, quand on connait les symboles de restes normiques de ce nombre par rapport aux corps composants, et la condition nécessaire et suffisante pour qu'il soit égal à 1 est que les symboles par rapport aux corps composants soient égaux à 1. De là résulte que *le corps composé de plusieurs corps relativement abéliens par rapport à k est corps de classes sur k pour la partie commune aux groupes associés aux corps composants.* En particulier, supposons que les groupes associés dans k aux deux sur-corps relativement abéliens K, K' soient égaux. Alors le groupe associé à KK' est encore le même groupe, et par suite $(KK' : k) = (K : k) = (K' : k)$, c'est-à-dire $K = K'$. *Nous avons donc démontré le théorème d'unicité de la théorie du corps de classes local.*

Lemme 6. *Si K est corps de classes sur k pour le groupe H, si H' est un groupe de nombres de k contenant H, le corps K contient un corps de classes K' sur k pour H'.*

Soit en effet K' le sous-corps de K appartenant au groupe des opérations $\left(\frac{\beta, K}{p}\right)$ pour les nombres β de H'. Ce groupe est d'ordre $(H' : H)$ et par suite $(K' : k) = (k^* : H')$. Comme d'autre part tout nombre de H' est, en vertu du théorème 9 (appliqué en prenant $Z = K'$), norme relative d'un nombre de K', le groupe associé à K' dans k contient H' et, ayant même indice que H', est H'.

Théorème 10. *Soit τ un isomorphisme de k avec un corps τk. K etant un sur-corps relativement abelien de k, τ se prolonge par un isomorphisme de K avec un corps τK dont le groupe de Galois par rapport à τk peut être considéré comme le transformé par τ du groupe de K par rapport à k. Si β est un nombre $\neq 0$ de k, on a*

$$\left(\frac{\tau\beta, \tau K/\tau k}{p_{\tau k}}\right) = \tau\left(\frac{\beta, K}{p}\right)\tau^{-1}.$$

Il suffit de démontrer le théorème dans le cas où K est cyclique par rapport à k. Soit s une substitution engendrant le groupe de K par rapport à k. Construisons l'algèbre (β, K, s). Elle contient un élément u tel que $u^n = \beta$ [si $n = (K : k)$], et que, pour tout élément x de K, $xu = ux^s$. De même dans l'algèbre $(\tau\beta, \tau K, \tau s \tau^{-1})$ il y a un élément u' tel que $u'^n = \tau\beta$ et que $\tau x \cdot u' = u' \cdot (\tau x)^{\tau s \tau^{-1}}$. Mettons un élément quelconque de la

première algèbre sous la forme $\sum_{i=0}^{n-1} x_i u^i$, les x_i étant des coefficients dans K, et associons à cet élément l'élément $\sum_{i=0}^{n-1} \tau x_i \cdot u'^i$ de la seconde algèbre. La correspondance entre les éléments des deux algèbres est biunivoque; à la somme de deux éléments correspond la somme des éléments correspondants; il en est de même pour les produits, comme on le voit en remarquant que à $u^h u^{h'}$ correspond $u'^h u'^{h'}$ et que à $ux = x^{s^{-1}} u$ correspond $\tau(x^{s^{-1}}) \cdot u' = (\tau x)^{\tau s^{-1} \tau^{-1}} \cdot u' = u' \cdot \tau x$. Par conséquent la correspondance ainsi définie est une isomorphie des deux algèbres. Or soit W le sur-corps non-ramifié de k de degré n : si $\left(\frac{\beta, K}{p}\right) = s^a$ la première algèbre est semblable à la puissance a-ième du corps gauche normé de centre k de degré n, et se met sous la forme (p^a, W, σ) où σ est l'inverse de la substitution de Frobenius $\left(\frac{W}{(p)}\right)$. Donc la seconde se met sous la forme $(\tau p^a, \tau W, \tau\sigma\tau^{-1})$. Or $\tau\sigma\tau^{-1}$ est l'invers de la substitution de Frobenius $\left(\frac{\tau W}{(\tau p)}\right)$, et par suite $\left(\frac{\tau\beta, \tau K/\tau k}{p}\right) = \tau s^a \tau^{-1}$ ce qui prouve le théorème.

Nous avons donc démontré les diverses propriétés connues du symbole de restes normiques. On peut chercher le symbole de restes normiques le plus général qui satisfasse aux théorèmes 1—10. On démontre facilement que ce symbole s'obtient de la manière suivante: soit $p_1, p_2, \ldots$ la suite des nombres premiers. Choisissons d'une manière quelconque pour chaque i un entier m_i premier à p_i; d'autre part soit K un sur-corps relativement abélien quelconque de k. Considérons K comme composé de corps K_i dont les degrés relatifs sont des puissances de nombres premiers p_i, ce qui est possible d'une seule manière. Le symbole de restes normiques le plus général est donné par la formule

$$\left(\frac{\beta, K}{p}\right)^* = \Pi \left(\frac{\beta, K_i}{p}\right)^{m_i}.$$

Ceci permet de démontrer que notre symbole est identique à celui défini dans H. 1. En effet, pour un sur-corps relativement cyclique non ramifié de k de degré p_i^x les deux symboles coïncident. Par suite les nombres m_i qui correspondent au symbole de M. Hasse, exprimé au moyen de celui ici défini, doivent être $\equiv 1 \pmod{p_i^x}$ quelque soit x, donc doivent être égaux à 1. Cette identité peut aussi se démontrer en remarquant qu'il résulte de H. 3 que, dans le cas cyclique, le symbole de M. Hasse satisfait aux conditions qui déterminent notre symbole.

VI. Le symbole de Hilbert.

Soit n un entier qui restera fixe. Nous allons considérer des corps de base k qui contiennent les racines primitives n-ièmes de l'unité ζ^i. Un sur-corps relativement cyclique de k de degré relatif diviseur de n sera alors de la forme $k(\sqrt[n]{\alpha})$ α étant un nombre de k. Nous pouvons alors définir le symbole de Hilbert: soient α, β deux nombres $\neq 0$ de k, et soit $K = k(\sqrt[n]{\alpha})$. Soit $\left(\frac{\beta, K}{p}\right) = s$. On a $s\sqrt[n]{\alpha} = \vartheta \cdot \sqrt[n]{\alpha}$, ϑ étant une racine n-ième de l'unité. On pose

$$\left(\frac{\beta, \alpha}{p}\right) = \vartheta.$$

Le symbole de Hilbert ainsi défini jouit de propriétés qui se déduisent facilement des théorèmes 1—10. Non n'insisterons pas sur l'énoncé de ces propriétés (Voir H. 4, II, p. 55). Par contre nous démontrerons la loi de permutation du symbole de Hilbert, qui n'a pas d'analogue dans la théorie du symbole de restes normiques:

Théorème 11. *α, β étant deux- nombres $\neq 0$ de k, on a*

$$\left(\frac{\alpha, \beta}{p}\right) \cdot \left(\frac{\beta, \alpha}{p}\right) = 1 \ ^{15}).$$

Supposons d'abord que les corps $k(\sqrt[n]{\alpha})$ et $k(\sqrt[n]{\beta})$ soient des sur-corps de degré n de k. Soit s une substitution engendrant le groupe de $k(\sqrt[n]{\alpha})$ par rapport à k, et soit $s\sqrt[n]{\alpha} = \zeta \cdot \sqrt[n]{\alpha}$. Soit $\mathfrak{R}$ le corps gauche normé de centre k de degré n. Supposons $\left(\frac{\beta, \alpha}{p}\right) = \zeta^a$, c'est-à-dire $\left(\frac{\beta, k(\sqrt[n]{\alpha})}{p}\right) = s^a$. Il en résulte $(\beta, k(\sqrt[n]{\alpha}), s) = \mathfrak{R}^a$. Mais ceci est équivalent au fait suivant: l'algèbre $k(u, v)$, définie par adjonction à k de deux éléments u, v satisfaisant aux relations

$$u^n = \alpha, \quad v^n = \beta, \quad v^{-1}uv = \zeta u,$$

est $\sim \mathfrak{R}^a$. Mais il en résulte tout de suite que l'algèbre définie par les relations

$$v^n = \beta, \quad u^n = \alpha, \quad u^{-1}vu = \zeta^{-1}v,$$

est $\sim \mathfrak{R}^a$, c'est-à-dire que $\left(\frac{\alpha, \beta}{p}\right) = \zeta^{-a}$, ce qui démontre le théorème dans le cas envisagé.

Passons au cas général. Il existe des nombres α_0, β_0 tels que les corps $k(\sqrt[n]{\alpha_0})$, $k(\sqrt[n]{\beta_0})$ soient de degré relatif n et que $\alpha = \alpha_0^d$, $\beta = \beta_0^{d'}$, d et d' étant des diviseurs de n. On a $\left(\frac{\beta, \alpha}{p}\right) = \left(\frac{\beta_0, \alpha}{p}\right)^d = \left(\frac{\beta_0, \alpha_0}{p}\right)^{dd'}$, comme il résulte de la règle $\left(\frac{\beta_0, k(\sqrt[n]{\alpha_0})}{p}\right) \to \left(\frac{\beta_0, k(\sqrt[n]{\alpha})}{p}\right)$, et par suite on est ramené au cas pour lequel la proposition est déjà démontrée.

VII. Le théorème d'existence.

Lemme 7. *k étant un corps contenant les racines n-ièmes de l'unité, H un sous-groupe de k^* tel que la puissance n-ième de tout nombre de k^* soit dans H, il existe un sur-corps relativement abélien de k corps de classes sur k pour le groupe H.*

En effet le groupe H contient le groupe H' des nombres qui sont n-ièmes puissances de nombres de k^*. En vertu du lemme 6, il suffit de démontrer qu'il existe un corps de classes sur k pour le groupe H'. Or soit K le corps déduit de k par adjonction des racines n-ièmes de tous les nombres de k. La théorie des corps kummériens montre que K est

---

[15]) La démonstration de ce théorème est entièrement analogue à celle donnée par M. Deuring, 1, du théorème suivant: k étant un corps parfait, a et b deux nombres de ce corps, si t est la plus petite puissance de a qui est norme relative d'un élément de $k(\sqrt[n]{b})$, ce nombre est aussi la plus petite puissance de b qui est norme relative d'un nombre de $k(\sqrt[n]{a})$.

composé de corps relativement cycliques par rapport à k dont les degrés relatifs divisent n et que $(K : k) = (k^* : H')$. Donc le groupe associé à K dans k contient toutes les puissances n-ièmes des nombres de k et, étant de même indice que H', se confond avec H'.

Théorème 12. *k étant un corps de nombres p-adiques, H un sous-groupe d'indice fini de k^*, il y a un sur-corps relativement abélien de k corps de classes sur k pour le groupe H.*

En effet, il y a un entier n tel que la n-ième puissance de tout nombre de k^* soit dans H. Soit k' le corps déduit de k par adjonction des racines n-ièmes de l'unité, et soit H' le groupe des nombres de k' dont la norme par rapport à k est dans H. La puissance n-ième de tout nombre $\neq 0$ de k' est dans H', et par suite (lemme 7) il y a un corps K' relativement abélien par rapport à k' corps de classes sur k' pour le groupe H'. Le groupe H' étant invariant par les automorphismes τ de k' par rapport à k, il résulte du théorème 10 et du théorème d'unicité que K' coïncide avec ses conjugués relatifs par rapport à k. D'autre part soit s une opération quelconque du groupe de K' par rapport à k' : il existe un nombre β de k' tel que

$$\left(\frac{\beta,\ K'/k'}{p_{k'}}\right) = s.$$

D'où, en vertu du théorème 10,

$$\left(\frac{\beta^\tau,\ K'/k'}{p_{k'}}\right) = \tau s \tau^{-1}.$$

Mais $\beta^{1-\tau}$, étant de norme 1 par rapport à k, est dans H', et par suite $s = \tau s \tau^{-1}$.

Or on peut intercaler entre k et k' une suite de corps k_i avec $k_0 = k$, $k_h = k'$ telle que k_{i+1} soit un sur-corps relativement cyclique de k_i. Soit H_i le groupe des nombres de k_i dont la norme par rapport à k tombe dans H. Démontrons que pour chaque i le corps K' contient un corps de classes K_i sur k_i pour le groupe H_i. En effet, la proposition est vraie pour $i = h$. Supposons la démontrée pour k_i $(i > 0)$. En raisonnant exactement comme on l'a fait plus haut pour K', on verra que K_i est un sur-corps relativement galoisien de k_{i-1} et que les opérations du groupe de K_i/k_i appartiennent au centre du groupe de K_i/k_{i-1}. Mais le centre d'un groupe ne peut être un sous-groupe à groupe quotient cyclique que s'il est identique au groupe [16]). Par suite K_i est un sur-corps relativement abélien de k_{i-1}. Il est donc corps de classes sur k_{i-1} pour un groupe evidemment contenu dans H_{i-1}. Le lemme 6 montre alors qu'il contient un corps K_{i-1} corps de classes sur k_{i-1} pour le groupe H_{i-1}. En particulier K_0 est le corps de classes sur k pour le groupe H.

VIII. Le théorème de translation pour des extensions quelconques.

Nous nous proposons de généraliser les théorèmes 5 et 9 au cas où Z est une extension finie quelconque de k:

Théorème 13. *Si Z est une extension quelconque finie de k, et si K est un sur-corps relativement abélien de k, on a, B étant un nombre $\neq 0$ de Z,*

$$\left(\frac{B,\ KZ/Z}{p_Z}\right) = \left(\frac{N_{Zk}(B),\ K}{p}\right).$$

1) Supposons que K soit un sur-corps relativement cyclique non ramifié de k. Soient f le degré relatif de (p_Z) par rapport à k, et $(p_Z)^a$ la contribution de (p_Z) à B. On a

[16]) En effet, s, s' représentant des opérations du centre et τ un élément tel que tout élément du groupe puisse se mettre sous la forme $\tau^l s$, les opérations $\tau^a s$, $\tau^b s'$ sont toujours permutables.

$$\left(\frac{B, KZ/Z}{pz}\right) = \left(\frac{KZ/Z}{(pz)}\right)^{-a}, \quad \left(\frac{N_{Zk}(B), K}{p}\right) = \left(\frac{K}{(p)}\right)^{-af},$$

et on sait que

$$\left(\frac{KZ/Z}{(pz)}\right) = \left(\frac{K}{(p)}\right)^{f},$$

ce qui démontre le théorème dans ce cas particulier.

2) Pour démontrer le théorème dans le cas général, il suffit evidemment de le démontrer quand K est cyclique par rapport à k. Soit $n = (K:k)$. Nous supposerons d'abord K et Z étrangers par rapport à k de sorte que $(KZ : Z) = n$. Soit W le sur-corps relativement cyclique non ramifié de k de degré n', n' étant choisi de manière à ce que $(WZ : Z) = n$. Prenons un nombre B_0 de Z primitif par rapport aux groupes associés dans Z aux sur-corps KZ et WZ [17]). On a $B = B_0^a \cdot N_{KZ,z}(\Gamma)$, Γ étant un nombre de KZ, d'où $N_{Zk}(B) = N_{Zk}(B_0^a) \cdot N_{KZ,k}(\Gamma)$, ce qui montre qu'il suffit de démontrer le théorème pour le nombre B_0.

Or posons

$$\left(\frac{B_0, KZ/Z}{pz}\right) = s, \left(\frac{B_0, ZW/Z}{pz}\right) = t.$$

Le nombre B_0 est norme relative par rapport à Z d'un nombre du sous-corps de ZKW appartenant au groupe engendré par $s't$. D'autre part soit $\left(\frac{N_{Zk}(B_0), K}{p}\right) = s'$. On a $\left(\frac{N_{Zk}(B_0), W}{p}\right) = t$, en vertu de la première partie de la démonstration, et par suite $N_{Zk}(B_0)$ est norme relative par rapport à k d'un nombre du sous-corps de KW appartenant au groupe engendré par $s't$. Mais il est aussi norme relative par rapport à k d'un nombre du sous-corps de KW appartenant au groupe engendré par st, car ce sous-corps est contenu dans le sous-corps de KZW appartenant au groupe engendré par st. Or les opérations st, $s't$ sont d'ordre n. Donc les corps des éléments qu'elles laissent invariants sont des sous-corps de KW sur lesquels KW est de degré n. Ils sont corps de classes sur k pour des groupes contenant le groupe H^*, associé a KW, comme sous-groupe d'indice n, et qui contiennent tous deux $N_{Zk}(B_0)$. Mais, B_0 étant primitif par rapport au groupe associé dans Z à WZ, la plus petite puissance de $N_{Zk}(B_0)$ qui est dans H^* est la puissance n-ième et par suite les sous-corps de KW appartenant aux groupes engendrés par st par $s't$ sont identiques; les ordres de s, t étant égaux à n (comme il résulte du choix de B_0), cela n'est possible que si $s = s'$, ce qui démontre le théorème dans le cas envisagé.

Passons maintenant au cas général, et soit $k' = [K, Z]$. En vertu de la première partie de la démonstration, on a

$$\left(\frac{B, KZ/Z}{pz}\right) = \left(\frac{N_{Zk'}(B), K/k'}{p_{k'}}\right)$$

et, en vertu du théorème 4, on a

---

[17]) Soient s, t des automorphismes primitifs de ZK/Z et de ZW/Z, qui produisent le même automorphisme de $[ZK, ZW]$. Il suffit de prendre un nombre B_0 tel que

$$\left(\frac{B_0, ZKW}{pz}\right) = st.$$

$$\left(\frac{N_{Zk'}(B),\ K/k'}{p_{k'}}\right) = \left(\frac{N_{Zk}(B),\ K}{p}\right),$$

ce qui démontre le théorème 13.

Il en résulte immédiatement que KZ est corps de classes sur Z pour le groupe des nombres de Z dont la norme par rapport à k est dans le groupe associé à K dans k.

Théorème 14. *Si Z est une extension finie de k, le groupe associé à Z dans k est le groupe associé dans k au plus grand sur-corps relativement abélien de k contenu dans Z.*

En effet, soit H le groupe associé à Z dans k et soit K corps de classes sur k pour le groupe H. KZ est corps de classes sur Z pour le groupe des nombres de Z dont la norme par rapport à k est dans H. Mais ce groupe contient tous les nombres de Z, et par suite K est contenu dans Z. Reciproquement, si K' est un sur-corps relativement abélien de k contenu dans Z, le groupe associé à K' dans k contient evidemment H, et par suite K' est contenu dans K.

IX. Le symbole de restes normiques dans un corps fini.

Dans ce paragraphe k représentera non plus comme jusqu'ici un corps de nombres p-adiques, mais un corps fini de nombres algèbriques. p représentera un idéal premier de ce corps.

Soit K un sur-corps relativement abélien de k, et soit P un facteur premier de p dans K. On désignera par k_p, K_P les corps de nombres p-adiques et P-adiques de k, K. β désignant un nombre $\neq 0$ de k, nous poserons

$$\left(\frac{\beta,\ K}{p}\right) = \left(\frac{\beta,\ K_P}{p}\right),$$

le symbole de restes normiques du second membre devant être calculé en regardant β comme un nombre de k_p.

1) *La condition nécessaire et suffisante pour que $\left(\frac{\beta,\ K}{p}\right) = 1$ est que β soit reste normique de K mod. p^n quelque soit n.*

En effet, on sait que la condition énoncée est encore la condition nécessaire et suffisante pour que β soit norme relative par rapport à k_p d'un nombre de K_P.

2) *Le symbole $\left(\frac{\beta,\ K}{p}\right)$ est un caractère du groupe des nombres $\neq 0$ de k.*

3) *Si K' est un corps compris entre k et K, on a*

$$\left(\frac{\beta,\ K}{p}\right) \to \left(\frac{\beta,\ K'}{p}\right).$$

4) *Si τ est un isomorphisme de k avec un corps τk, qui se prolonge par un isomorphisme de K avec un corps τK dont le groupe par rapport à τk peut être considéré comme transformé par τ du groupe de K par rapport à k, on a*

$$\left(\frac{\tau\beta,\ \tau K/\tau k}{\tau p}\right) = \tau\left(\frac{\beta,\ K}{p}\right)\tau^{-1}.$$

Les propositions 2), 3), 4) se déduisent immédiatement des théorèmes 7, 8, 10.

5) *Si Z est une extension finie de k, soient q_i les divers facteurs premiers de p dans Z. B étant un nombre $\neq 0$ de Z, on a*

$$\prod_i \left(\frac{B,\ KZ/Z}{q_i}\right) = \left(\frac{N_{Zk}(B),\ K}{p}\right).$$

En effet considérons Z comme un système hypercomplexe par rapport à k, et formons, au sens de l'extension des systèmes hypercomplexes, l'extension Z_p, produit direct de Z et de k_p. On sait que Z_p est somme directe des corps de nombres q_i-adiques de Z [18]). Or la norme d'un nombre d'une somme directe est le produit des normes des composants du nombre dans les divers termes. Par suite

$$\left(\frac{N_{Zk}(B),\ K}{p}\right) = \left(\frac{N_{Zk}(B),\ K_P}{p}\right) = \prod_i \left(\frac{N_{Z_{q_i}k_p}(B),\ K_P}{p}\right).$$

Or, en vertu du théorème 13, on a

$$\left(\frac{N_{Z_{q_i}k_p}(B),\ K_P}{p}\right) = \left(\frac{B,\ K_P Z_{q_i}/Z_{q_i}}{q_i}\right).$$

Comme de plus on a

$$\left(\frac{B,\ K_P Z_{q_i}/Z_{q_i}}{q_i}\right) = \left(\frac{B,\ KZ/Z}{q_i}\right),$$

la proposition 5) est démontrée.

[18]) En effet, si $f(x) = 0$ est l'equation irreductible à laquelle satisfait dans k un nombre de Z, $f(x)$ se décompose dans k_p en un produit de facteurs irreductibles $f_i(x)$, et les equations $f_i(x) = 0$ sont les equations irreductibles auxquelles satisfont dans k_p des nombres engendrant les Z_{q_i}. La proposition résulte alors de la note (5).

Eingegangen 29. Mai 1932.

On certain exponential sums.

By *H. Davenport* in Cambridge.

Introduction.

1. This paper is concerned with exponential sums of the form

$$S_f = \sum_{x=0}^{p-1} e(f(x)), \qquad e(t) = e^{\frac{2t\pi i}{p}},$$

where p is a prime and $f(x)$ a polynomial in x (or more generally a rational function of x, in which case the rational zeros of the denominator are excluded from the summation), whose coefficients are integers taken modulo p. If f is a quadratic, the sum is a Gaussian sum, and has absolute value $\sqrt{p}$. More generally, if f is of the form $a(x+b)^m$, the sum is zero unless $n = (m, p-1) > 1$, in which case it is

$$\bar{\chi}_1(a)\,\tau(\chi_1) + \cdots + \bar{\chi}_{n-1}(a)\,\tau(\chi_{n-1}),$$

where $\chi_1, \ldots, \chi_{n-1}$ are those non-principal Dirichlet characters mod. p having for their n-th power the principal character, and

$$\tau(\chi) = \sum_{x=1}^{p-1} \chi(x)\, e(x).$$

It is well known that $|\tau(\chi)| = \sqrt{p}$, hence S_f is again $O(\sqrt{p})$ for large primes p.

Apart from these special cases, the order of magnitude of S_f for large p is unknown. In a recent paper [1]) Mordell has proved, firstly, that if f is a polynomial of degree n then

$$S_f = O(p^{1-\frac{1}{n}}), \text{ [2]}) \tag{1}$$

and secondly that if g is of the form

$$a_1 x^{l_1} + a_2 x^{l_2} + \cdots + a_n x^{l_n} \text{ [3]})$$

then

$$S_g = O(p^{1-\frac{1}{2n}}). \tag{2}$$

The object of this paper is to improve on these results in certain cases, and to give some curious relations connecting various special types of exponential sum.

As regards (1) I shall prove that when f is a cubic,

$$S_f = O(p^{\frac{5}{8}}), \tag{3}$$

---

[1]) L. J. Mordell, "On a sum analogous to a Gauss's sum", Oxford Quarterly Journal 3 (1932), 161—167.

[2]) All assertions of this type are to be understood as being uniform in the coefficients of the polynomials involved. That is to say, the constants implied by the symbol O depend only on the *powers* occurring in the polynomials. It is also assumed tacitly in (1), (2), ..., (6) that the polynomials concerned are not constants.

[3]) The l's are any positive or negative integers; the use of negative powers modulo p presents no difficulty. If any of the l's are negative, the lower limit of summation is to be read 1 instead of 0.

and that when f is of degree n $(\geqq 4)$,

$$S_f = O(p^{1-\frac{1}{m}}), \tag{4}$$

where m is the largest integer of either of the forms 2^γ, $3 \cdot 2^\gamma$ not exceeding n. Thus (4) is an improvement on (1) except when n is of the form $2^\gamma (g \geqq 2)$ or $3 \cdot 2^\gamma (g \geqq 1)$.

As regards (2) I shall prove that for any fixed n other than zero

$$\sum_{x=0}^{p-1} e(a x^n + b x^{2n}) = O(p^{\frac{5}{8}}), \tag{5}$$

and

$$\sum_{x=1}^{p-1} e(ax^n + bx^{-n}) = O(p^{\frac{2}{3}}). \tag{6}$$

When $n = 1$, the sum in (6) is a Kloosterman sum [1]), and Herr Salié of Leipzig informs me that he proved this inequality for Kloosterman sums some months ago. [2])

Several of these inequalities will be established for partial as well as complete sums. I shall also prove the following inequality:

$$|\sum_{x_1}^{x_2} \chi(ax^2 + bx + c)| < Kp^{\frac{2}{3}} \log p, \qquad (0 \leqq x_1 \leqq x_2 \leqq p), \tag{7}$$

where χ is any non-principal Dirichlet character mod. p, K an absolute constant, and $a \not\equiv 0 \pmod p$.

I wish to take this opportunity of expressing my gratitude to Prof. Mordell, not only for suggesting many of these problems to me in the first place but also for much valuable encouragement and advice.

Notation.

2. We make free use of fractional expressions which are to be interpreted modulo p; the context will decide in each case whether this interpretation is implied or not. All congruences are modulo p, unless the contrary is explicitly stated.

We use $\sum_x$ to denote summation over any set of p mutually incongruent numbers, and $\sum_x'$ to denote summation over such a set excluding $x \equiv 0$.

As regards the Legendre symbol of quadratic residuacity, it is convenient to adopt the convention $\left(\frac{0}{p}\right) = 0$. The following obvious identity may be stated here for reference: *whatever function* φ *(defined for all* x *modulo* p*) may be,*

$$\sum_x \varphi(x^2) = \sum_x \varphi(x) + \sum_x \left(\frac{x}{p}\right) \varphi(x). \tag{8}$$

In dealing with the sums (5) and (6) we may suppose that n is a divisor of $p - 1$. For if $n = m\delta$, where $\delta = (n, p-1)$, the congruence $x^n \equiv y$ has precisely the same number of solutions in x as the congruence $x^\delta \equiv y$. [3]) Hence the sums (5) and (6) are the same as the corresponding sums with n replaced by δ, which is a divisor of $p - 1$.

---

[1]) These arise in the applications of the Hardy-Littlewood method as modified by Kloosterman. For references see H. Salié, "Über die Kloostermanschen Summen", Math. Zeitschrift 34 (1931), p. 91.

[2]) His proof is in course of publication in the Math. Zeitschrift. The previously known result was $O(p^{\frac{3}{4}})$. The improvement gives at once a corresponding improvement in the error terms in the results of Kloosterman and Estermann.

[3]) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie (1879), p. 71.

Now if n is any divisor of $p-1$, there exist n Dirichlet characters, say $\chi_0, \chi_1, \cdots, \chi_{n-1}$ (χ_0 being the principal character) for which $\chi^n = \chi_0$, and the expression

$$\chi_0(y) + \chi_1(y) + \cdots + \chi_{n-1}(y)$$

has for any $y \not\equiv 0$ the value n or 0 according as y is or is not an n-th power residue; that is, is equal to the number of solutions in x of $x^n \equiv y$. Thus we have the following generalisation of (8):

$$\sum_x{}' \varphi(x^n) = \sum_{j=0}^{n-1} \sum_y{}' \chi_j(y)\, \varphi(y). \tag{9}$$

In particular,

$$\sum_x{}' e(ax^n + bx^{2n}) = \sum_{j=0}^{n-1} \sum_y{}' \chi_j(y)\, e(ay + by^2), \tag{10}$$

$$\sum_x{}' e(ax^n + bx^{-n}) = \sum_{j=0}^{n-1} \sum_y{}' \chi_j(y)\, e(ay + by^{-1}). \tag{11}$$

The cubic sum.

3. Theorem 1. $\sum_x e(ax^3 + bx^2 + cx) = O(p^{\frac{5}{6}})$, $(a \not\equiv 0)$.

Proof: We can suppose without loss of generality that $b = 0$; the general case reduces to this on writing $x - \frac{b}{3a}$ for x. Denoting the sum by $Q = Q(a, c)$ we have

$$Q^2 = \sum_x \sum_y e(ax^3 + ay^3 + cx + cy).$$

Making the (1, 1) transformation

$$x + y \equiv 2\eta, \quad x - y \equiv 2\xi, \tag{12}$$

we obtain

$$Q^2 = \sum_\eta \sum_\xi e(6a\xi^2\eta + 2a\eta^3 + 2c\eta).$$

The sum over ξ is a Gaussian sum, and has the value

$$\left(\frac{6a\eta}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}$$ [1])

unless $\eta \equiv 0$, in which case it has the value p. Hence

$$Q^2 = p + \left(\frac{6a}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}\, R(a, c), \tag{13}$$

where

$$R(a, c) = \sum_x \left(\frac{x}{p}\right) e(2ax^3 + 2cx).$$

It follows from (13) that the theorem will be proved if we prove that $R = O(p^{\frac{3}{4}})$. There are many ways of doing this; perhaps the simplest is to deduce it from (2). By (8),

$$\sum_x e(2ax^6 + 2cx^2) = \sum_x e(2ax^3 + 2cx) + \sum_x \left(\frac{x}{p}\right) e(2ax^3 + 2cx).$$

The sum on the left, and the first sum on the right are each $O(p^{\frac{3}{4}})$ by (2), and the result follows. [2])

---

[1]) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie (1879), p. 296.

[2]) A more direct method of proving that $R = O(p^{\frac{3}{4}})$ is to apply the transformation (12) to R^2 and then replace ξ by $\eta\xi$. On finds that R^2 is expressible as a linear combination with coefficients ± 1 of Q's with varying a. The

The sum with a general polynomial.

4. This section is concerned with a lemma of a general character on polynomials, for the proof of which I am indebted to the kindness of Prof. van der Waerden.

We first recall some familiar propositions of algebra. They are valid for polynomials whose coefficients belong to any "Körper", in particular if they are integers taken to modulus p.

Given r polynomials $f_1, \ldots, f_r$ in one variable, there exists a "system of resultants" $D_1, \ldots, D_h$ consisting of polynomials in the coefficients of $f_1, \ldots, f_r$ such that the vanishing of all of the D's is the necessary and sufficient condition that *either* the f's have a common factor, *or* all the coefficients of the formally highest terms [1]) in the f's vanish. For two polynomials f_1, f_2 of degrees n_1, n_2, the system consists of a single resultant, which is of degree n_2 in the coefficients of f_1 and n_1 in the coefficients of f_2. For several polynomials, all of degree not exceeding n the degree of each of the D's does not exceed $2n$. [2]) If $f_1, \ldots, f_r$ are polynomials in two variables x, y, and each resultant of the system of resultants with respect to x vanishes identically in y, then $f_1, \ldots, f_r$ have a common factor.

Lemma 1. *Suppose $f(x, y)$, $g(x, y)$ are two polynomials in x, y of degrees m, n whose Jacobian*

$$\begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial g}{\partial x} \\ \frac{\partial f}{\partial y} & \frac{\partial g}{\partial y} \end{vmatrix}$$

is not identically congruent to zero mod. p. Then there are not more than $2mn$ pairs of values of a, b for which the congruences

$$\text{(14)} \qquad \begin{cases} f(x, y) \equiv a \pmod p \\ g(x, y) \equiv b \pmod p \end{cases}$$

have more than mn solutions in x, y.

Proof: We can suppose that in f the term cy^m with $c \not\equiv 0$ occurs; for if not we can achieve this by making a transformation in x of the form $x = x' + ky$. [3]) Let the resultant of $f(x, y) - a$, $g(x, y) - b$ with respect to y be

$$R(x, a, b) = \sum_{\nu=0}^{l} q_\nu(a, b) x^\nu ,$$

where the q_ν are polynomials in a, b of degrees not more than n in a and m in b. Then the congruences (14) have not more than mn solutions in x, y except for those values of a, b which satisfy all the congruences

$$\text{(15)} \qquad q_\nu(a, b) \equiv 0 \pmod p , \qquad \nu = 0, 1, \ldots, l.$$

We shall show that if the polynomials q_ν have a common divisor $q(a, b)$ mod. p, then the Jacobian of f, g is identically congruent to zero, contrary to hypothesis. For if we replace a by an indeterminate u, and b by a root v of the equation $q(u, v) = 0$

---

result now follows by Cauchy's (Schwarz's) inequality from the easily-proved fact that

$$\sum_a |Q|^2 = O(p^2) .$$

[1]) That is, the highest term which *can* occur, supposing the coefficients to be functions of other variables.

[2]) See the method of definition of the system of resultants in van der Waerden's Moderne Algebra, Zweiter Teil (1931), § 73.

[3]) It is assumed here that $m < p$, but if $m \geqq p$ and $n \geqq p$ the lemma is trivial.

taken in an algebraic field $\mathsf{P}(u, v)$ over the field of rational functions of u with coefficients mod. p, then we have $q_\nu(u, v) = 0$, $R(x, u, v) = 0$, and therefore the polynomials $f(x, y) - u$, $g(x, y) - v$ have a common factor $d(x, y) = d(x, y; u, v)$ depending rationally on u, v. From

$$f(x, y) \equiv u \pmod{d(x, y)},$$
$$g(x, y) \equiv v \pmod{d(x, y)},$$
$$q(u, v) = 0$$

we have

$$q(f(x, y),\ g(x, y)) \equiv 0 \pmod{d(x, y)};$$

that is, $d(x, y, u, v)$ is a divisor of $q(f(x, y),\ g(x, y))$ both considered as polynomials in x, y over the field $\mathsf{P}(u, v)$. Now $q(f, g)$ is a polynomial in x, y independent of u and v, which, if it is not identically congruent to zero, can be expressed as a product of absolutely irreducible polynomials in one and only one way (apart from changes in the order of the factors). Hence $d(x, y)$ as a factor of $q(f, g)$ must be independent of u and v. But it is evident that $f(x, y) - u$ has no factor independent of u. Thus it must be that $q(f, g)$ is identically zero in x, y, from which it follows that the Jacobian is identically zero.

We have therefore proved that the polynomials $q_\nu(a, b)$ have no common divisor. If we eliminate b from the polynomials q_ν we obtain a system of resultants

$$r_1(a), \ldots, r_h(a),$$

which are polynomials in a at least one of which is not identically zero. Each polynomial r is of degree not more than $2mn$. Hence there are not more than $2mn$ pairs of values of a, b satisfying all the congruences $q_\nu(a, b) \equiv 0$. [1]) This proves the lemma.

5. We now make use of this lemma in connection with polynomials of a certain special type. Let $f(x) = a_n x^n + \cdots + a_0$, $a_n \not\equiv 0$, be a polynomial of degree n. We construct from f the following polynomials:

$$f_{y_1}(x) = f(y_1(1 + \sqrt{x})) + f(y_1(1 - \sqrt{x})), \tag{16}$$

$$f_{y_1, y_2}(x) = f_{y_1}(y_2(1 + \sqrt{x})) + f_{y_1}(y_2(1 - \sqrt{x})), \tag{17}$$

and generally

$$f_{y_1, \ldots, y_r}(x) = f_{y_1, \ldots, y_{r-1}}(y_r(1 + \sqrt{x})) + f_{y_1, \ldots, y_{r-1}}(y_r(1 - \sqrt{x})). \tag{18}$$

Obviously $f_{y_1, \ldots, y_r}(x)$ is a polynomial of degree $n_r = \left[\frac{n}{2^r}\right]$ in x whose coefficients are polynomials in $y_1, \ldots, y_r$, so that we may write

$$f_{y_1, \ldots, y_r}(x) = H_0 + H_1 x + \cdots + H_{n_r} x^{n_r},$$
$$H_i = H_i(y_1, \ldots, y_r).$$

The coefficients in the polynomials H are linear combinations of $a_0, a_1, \ldots, a_n$ with numerical coefficients [2]), and moreover it is easily seen that H_i involves only

$$a_{2^r i},\ a_{2^r i + 1},\ \ldots,\ a_n. \tag{19}$$

---

[1]) Values of a to which more than one value of b correspond occur a corresponding number of times as zeros of the system of resultants $r_1(a), \ldots, r_h(a)$.

[2]) That is, integers depending only on n and r. We can always suppose that p is greater than all such numerical coefficients.

Throughout what follows we suppose $r \geqq 2$ and $n_r \geqq 2$. We are concerned particularly with the behaviour of H_1, H_2, regarded as polynomials in y_1, y_2 for fixed $y_3, \ldots, y_r$. Suppose none of $y_3, \ldots, y_r$ is congruent to zero, and consider the congruences

$$H_1(y_1, y_2) \equiv h_1 , \tag{20}$$

$$H_2(y_1, y_2) \equiv h_2 . \tag{21}$$

For arbitrary values of h_1, h_2 the number of solutions of these congruences in y_1, y_2 does not exceed the product of their degrees. These degrees depend only on n, r, and since we suppose $n_r \geqq 2$, so that $2^{r+1} \leqq n$, the number of solutions of (20), (21) for arbitrary h_1, h_2 does not exceed a number depending only on n, that is, it is $O(1)$.

There may be exceptional values of h_1, h_2 for which this is not so. It is essential for our purposes to find an upper bound for the number of such values. This we do in the following lemma:

Lemma 2. *If $y_3, \ldots, y_r$ have any values none of which is congruent to zero, there are only $O(1)$ exceptional sets of values of h_1, h_2 for which the congruences* (20), (21) *have more than $O(1)$ solutions in y_1, y_2 with $y_1 \not\equiv 0$, $y_2 \not\equiv 0$. For these exceptional values of h_1, h_2 the number of solutions is $O(p)$.*

Proof: Since we are concerned only with y_1, y_2 neither of which is congruent to zero, we are at liberty to write y for y_1 and z for $y_1^2 y_2$ and prove the lemma for the number of solutions in y, z. We have from (16), (17),

$$\left\{ \frac{1}{2} f_{y_1}(x) = f(y) + xy^2 \frac{f''(y)}{2!} + x^2 y^4 \frac{f^{(4)}(y)}{4!} + \cdots = \sum_{m,l} \binom{l}{2m} a_l y^l x^m , \right. \tag{22}$$

where the summation is over $0 \leqq 2m \leqq l \leqq n$; and

$$\frac{1}{4} f_{y_1, y_2}(x) = \sum_{m,l} \binom{l}{2m} z^l x^m \frac{f^{(2l)}(y)}{(2l)!} , \tag{23}$$

where the summation is over $0 \leqq 2m \leqq l \leqq n_1 = \left[\frac{n}{2}\right]$. Thus the coefficient of x^m in $f_{y_1, y_2}(x)$ is a linear combination of $z^l f^{(2l)}(y)$ with $2m \leqq l \leqq n_1$. Regarding $f_{y_1, y_2}(x)$ as the polynomial from which $f_{y_1, \ldots, y_r}(x)$ is derived instead of $f(x)$ it follows from (19) with r replaced by $r-2$ and i by 1 or 2 that H_1, H_2 have the forms

$$H_1 = \alpha_{2^{r-1}} z^{2^{r-1}} f^{(2^r)}(y) + \alpha_{2^{r-1}+1} z^{2^{r-1}+1} f^{(2^r+2)}(y) + \cdots + \alpha_{n_1} z^{n_1} f^{(2n_1)}(y) , \tag{24}$$

$$H_2 = \beta_{2^r} z^{2^r} f^{(2^{r+1})}(y) + \beta_{2^r+1} z^{2^r+1} f^{(2^{r+1}+2)}(y) + \cdots + \beta_{n_1} z^{n_1} f^{(2n_1)}(y) , \tag{25}$$

where the α's and β's are polynomials in $y_3, \ldots, y_r$.

By lemma 1, it suffices to prove that the Jacobian of $H_1(y, z)$, $H_2(y, z)$ is not identically zero in y, z. This Jacobian is

$$\{2^{r-1}\alpha_{2^{r-1}} z^{2^{r-1}-1} f^{(2^r)}(y) + \cdots + n_1 \alpha_{n_1} z^{n_1-1} f^{(2n_1)}(y)\}\{\beta_{2^r} z^{2^r} f^{(2^{r+1}+1)}(y) + \cdots + \beta_{n_1} z^{n_1} f^{(2n_1+1)}(y)\}$$
$$- \{2^r \beta_{2^r} z^{2^r-1} f^{(2^{r+1})}(y) + \cdots + n_1 \beta_{n_1} z^{n_1-1} f^{(2n_1)}(y)\}\{\alpha_{2^{r-1}} z^{2^{r-1}} f^{(2^r+1)}(y) + \cdots + \alpha_{n_1} z^{n_1} f^{(2n_1+1)}(y)\}.$$

The coefficient of the term of lowest degree in z is

$$2^{r-1}\alpha_{2^{r-1}} f^{(2^r)}(y)\beta_{2^r} f^{(2^{r+1}+1)}(y) - 2^r \beta_{2^r} f^{(2^{r+1})}(y)\ \alpha_{2^{r-1}} f^{(2^r+1)}(y) .$$

We shall show that this is not identically zero in y. The coefficient of the highest power of y in it is

$$2^{r-1}\alpha_{2^{r-1}}\beta_{2^r}\{n(n-1)\cdots(n-2^r+1)\ n(n-1)\cdots(n-2^{r+1}) \tag{26}$$
$$- 2n(n-1)\cdots(n-2^{r+1}+1)\ n(n-1)\cdots(n-2^r)\}\, a_n .$$

It will suffice to prove that this is not congruent to zero.

Firstly, $\alpha_{2^r-1} \not\equiv 0$. Referring back to the way in which $f_{y_1,\dots,y_r}(x)$ is derived from $f_{y_1,y_2}(x)$ it is clear that the first term in the expression (24) of H_1 is derived entirely from the term

$$z^{2^r-1}x^{2^r-2}\frac{f^{(2^r)}(y)}{(2^r)!}$$

in the expression (23) of $\frac{1}{4}f_{y_1,y_2}(x)$. For any other term of the form

$$\binom{2^r-1}{2m}z^{2^r-1}x^m\frac{f^{(2^r)}(y)}{(2^r)!}$$

in (23) has $m < 2^{r-2}$ and therefore will not appear in the coefficient of x in $f_{y_1,\dots,y_r}(x)$. Hence

$$\alpha_{2^r-1} = \frac{4}{(2^r)!} \times \text{coefficient of } x \text{ in } (x^{2^r-2})_{y_3,\dots,y_r},$$

where by $(x^{2^r-2})_{y_3,\dots,y_r}$ we mean $\varphi_{y_3,\dots,y_r}(x)$ where $\varphi(x)$ is x^{2^r-2}. Now

$$(x^{2^r-2})_{y_3,\dots,y_r} = y_3^{2^r-2}\{(1+\sqrt{x})^{2^r-2} + (1-\sqrt{x})^{2^r-2}\}_{y_4,\dots,y_r},$$

and a term in x can only arise in this if we take the highest power of x inside the $\{\}$. Hence

$$\alpha_{2^r-1} = \frac{4}{(2^r)!}\,2y_3^{2^r-2} \times \text{coefficient of } x \text{ in } (x^{2^r-3})_{y_4,\dots,y_r} = \frac{2^r}{(2^r)!}\,y_3^{2^r-2}\cdots y_r^2,$$

by induction. β_{2^r} can be determined in precisely the same way, and we have

$$\beta_{2^r} = \frac{2^r}{(2^{r+1})!}\,y_3^{2^r-1}\cdots y_r^4.$$

Hence neither α_{2^r-1} nor β_{2^r} is congruent to zero. The remaining factor in (26) is

$$n(n-1)\cdots(n-2^r+1)n(n-1)\cdots(n-2^{r+1}+1)\{(n-2^{r+1})-2(n-2^r)\} \not\equiv 0.$$

This completes the proof of lemma 2. The last sentence in the enunciation follows from the fact that whatever value ($\not\equiv 0$) is given to z there are only $O(1)$ values of y for which either of (20), (21), say (20), is satisfied, since $\alpha_{2^r-1} \not\equiv 0$ and $f^{(2^r)}(y)$ is not identically zero and is of higher degree than

$$f^{(2^r+2)}(y), \dots, f^{(2n_1)}(y).$$

6. Lemma 3. *If $\varepsilon(x)$ is any function of x with absolute value not exceeding some absolute constant, then*

$$\sum_{A_1}\cdots\sum_{A_n}\Big|\sum_x \varepsilon(x)\,e(A_nx^n+\cdots+A_1x)\Big|^{2n} = O(p^{2n}). \tag{27}$$

Proof: This lemma is a trivial variation on what is proved by Mordell. [1]) The left side of (27) is equal to

$$p^n\Sigma\varepsilon(x_1)\cdots\varepsilon(x_n)\bar{\varepsilon}(y_1)\cdots\bar{\varepsilon}(y_n)$$

summed over all solutions of

$$x_1^i + x_2^i + \cdots + x_n^i \equiv y_1^i + y_2^i + \cdots + y_n^i \qquad (i = 1, 2, \dots n), \tag{28}$$

and since the number of solutions of the congruences (28) is $O(p^n)$ we have the result stated.

---

[1]) loc. cit., equation (11).

Lemma 4. *If*

$$T = \sum_x \left(\frac{(x-d_1)\cdots(x-d_\nu)}{p}\right) e(f(x)),$$

then

$$T^2 = \sum_y{}' \sum_x \left(\frac{(-1)^\nu\left(x-\delta\left(\frac{d_1}{y}\right)\right)\cdots\left(x-\delta\left(\frac{d_\nu}{y}\right)\right)}{p}\right) e(f_y(x))$$

$$+ \sum_y{}' \sum_x \left(\frac{(-1)^\nu x\left(x-\delta\left(\frac{d_1}{y}\right)\right)\cdots\left(x-\delta\left(\frac{d_\nu}{y}\right)\right)}{p}\right) e(f_y(x)) + O(p),$$

where

$$\delta(t) = (1-t)^2.$$

Proof: Apply to T^2 the transformation (12). We obtain

$$T^2 = \sum_\xi \sum_\eta \left(\frac{(\eta^2-\xi^2-2\eta d_1+d_1^2)\cdots(\eta^2-\xi^2-2\eta d_\nu+d_\nu^2)}{p}\right) e(f(\eta+\xi)+f(\eta-\xi)).$$

In the terms for which $\eta \not\equiv 0$, replace ξ by $\eta\xi$. Then

$$T^2 = \sum_\eta{}' \sum_\xi \left(\frac{(-1)^\nu\left(\xi^2-\delta\left(\frac{d_1}{\eta}\right)\right)\cdots\left(\xi^2-\delta\left(\frac{d_\nu}{\eta}\right)\right)}{p}\right) e(f_\eta(\xi^2)) + O(p).$$

The result follows on applying to this the identity (8).

7. Theorem 2. *If $f(x)$ is a polynomial of degree $n \geqq 4$, then*

$$\sum_x e(f(x)) = O(p^{1-\frac{1}{m}}),$$

where m is the largest number of either of the forms 2^q, $3\cdot 2^q$ which does not exceed n.

Proof: Denoting the sum in question by S, we have by lemma 4 with $\nu = 0$ [1]),

$$|S|^2 \leqq \sum_{y_1}{}' \left|\sum_x e(f_{y_1}(x))\right| + \sum_{y_1}{}' \left|\sum_x \left(\frac{x}{p}\right) e(f_{y_1}(x))\right| + O(p). \tag{29}$$

This is the first of a series of inequalities obtained by repeated application of lemma 4, and the use of Cauchy's (Schwarz's) inequality at the intermediate stages. By two applications of Cauchy's inequality to (29),

$$|S|^4 \leqq 3\left\{\sum_{y_1}{}' \left|\sum_x e(f_{y_1}(x))\right|\right\}^2 + 3\left\{\sum_{y_1}{}' \left|\sum_x \left(\frac{x}{p}\right) e(f_{y_1}(x))\right|\right\}^2 + O(p^2)$$

$$\leqq 3p\sum_{y_1}{}' \left|\sum_x e(f_{y_1}(x))\right|^2 + 3p\sum_{y_1}{}' \left|\sum_x \left(\frac{x}{p}\right) e(f_{y_1}(x))\right|^2 + O(p^2),$$

and again using lemma 4,

$$|S|^4 \leqq 3p\sum_{y_1}{}'\sum_{y_2}{}' \left|\sum_x e(f_{y_1,y_2}(x))\right| + 3p\sum_{y_1}{}'\sum_{y_2}{}' \left|\sum_x \left(\frac{x}{p}\right) e(f_{y_1,y_2}(x))\right|$$

$$+ 3p\sum_{y_1}{}'\sum_{y_2}{}' \left|\sum_x \left(\frac{x-1}{p}\right) e(f_{y_1,y_2}(x))\right| + 3p\sum_{y_1}{}'\sum_{y_2}{}' \left|\sum_x \left(\frac{x(x-1)}{p}\right) e(f_{y_1,y_2}(x))\right| + O(p^3).$$

---

[1]) that is, with no numbers d.

This is the second inequality of the series. It will be seen that the various factors preceeding $e(f_{y_1,y_2}(x))$ are the 4 possible combinations obtainable by taking any or none of $\left(\frac{x}{p}\right)$, $\left(\frac{x-1}{p}\right)$. At the third stage we shall clearly have the 8 possible combinations obtainable by taking any or none of

$$\left(\frac{x}{p}\right), \quad \left(\frac{x-1}{p}\right), \quad \left(\frac{x-\delta\left(\frac{1}{y_3}\right)}{p}\right)$$

and at the fourth stage, of

$$\left(\frac{x}{p}\right), \quad \left(\frac{x-1}{p}\right), \quad \left(\frac{x-\delta\left(\frac{1}{y_4}\right)}{p}\right), \quad \left(\frac{x-\delta\left(\frac{\delta\left(\frac{1}{y_3}\right)}{y_4}\right)}{p}\right),$$

and so on.

The general inequality, which may be immediately established by induction, is

$$(30) \qquad |S|^{2^r} \leqq C_r p^{2^r-r-1} \sum_{j=1}^{2^r} \sum_{y_1}' \cdots \sum_{y_r}' \left|\sum_x \varepsilon_j(x; y_3, \ldots, y_r)\, e(f_{y_1,\ldots,y_r}(x))\right| + O(p^{2^r-1}),$$

where C_r depends only on r, and the factors $\varepsilon_j(x)$ where j runs from 1 to 2^r are the 2^r possible combinations of

$$\left(\frac{x}{p}\right), \quad \left(\frac{x-1}{p}\right), \quad \left(\frac{x-\delta_3}{p}\right), \ldots, \left(\frac{x-\delta_r}{p}\right),$$

in which

$$\delta_r = \delta\left(\frac{1}{y_r}\right), \quad \delta_{r-1} = \delta\left(\frac{\delta\left(\frac{1}{y_{r-1}}\right)}{y_r}\right), \quad \delta_{r-2} = \delta\left(\frac{\delta\left(\frac{\delta\left(\frac{1}{y_{r-2}}\right)}{y_{r-1}}\right)}{y_r}\right),$$

and so on. All that it is necessary to observe is that ε is independent of y_1, y_2.

The proof of the theorem differs slightly according as $4 \leqq n \leqq 7$, or $n \geqq 8$.

Case 1 $(4 \leqq n \leqq 7)$. We require only (29). $f_y(x)$ is a polynomial of degree $n_1 = \left[\frac{n}{2}\right] = 2$ or 3. Let $\varepsilon(x)$ denote either of 1, $\left(\frac{x}{p}\right)$. We have

$$\sum_y' \left|\sum_x \varepsilon(x)\, e(f_y(x))\right| = \sum_y' \left|\sum_x \varepsilon(x)\, e\left(\frac{2y^2 f''(y)}{2!}x + \frac{2y^4 f^{(4)}(y)}{4!}x^2 + \cdots\right)\right|$$

$$= \sum_{\substack{y \\ f''(y)\not\equiv 0}}' \left|\sum_x \varepsilon(x)\, e\left(x + \frac{x^2}{4!}\frac{2f^{(4)}(y)}{(f''(y))^2} + \cdots + \frac{x^{n_1}}{(2n_1)!}\frac{2f^{(2n_1)}(y)}{(f''(y))^{2n_1}}\right)\right| + O(p),$$

on replacing x by $\frac{x}{y^2 f''(y)}$ in the terms for which $f''(y) \not\equiv 0$. By Hölder's inequality this is

$$\leqq p^{1-\frac{1}{2n_1}}\left\{\sum_{\substack{y \\ f''(y)\not\equiv 0}}' \left|\sum_x \varepsilon(x)\, e\left(x + \frac{x^2}{4!}\frac{2f^{(4)}(y)}{(f''(y))^2} + \cdots + \frac{x^{n_1}}{(2n_1)!}\frac{2f^{(2n_1)}(y)}{(f''(y))^{2n_1}}\right)\right|^{2n_1}\right\}^{\frac{1}{2n_1}} + O(p)$$

$$(31) \qquad \leqq p^{1-\frac{1}{2n_1}}\{10 \sum_{A_2} \cdots \sum_{A_{n_1}} \left|\sum_x \varepsilon(x)\, e(x + A_2 x^2 + \cdots + A_{n_1} x^{n_1})\right|^{2n_1}\}^{\frac{1}{2n_1}} + O(p),$$

since for any given A_2 the congruence $\frac{f^{(4)}(y)}{(f''(y))^2} \equiv 12\,A_2$ has not more than 10 solutions.

Now by lemma 3,

$$\sum_{A_1} \dots \sum_{A_{n_1}} \Big| \sum_x \varepsilon(x) e(A_1 x + \dots + A_{n_1} x^{n_1}) \Big|^{2n_1} = O(p^{2n_1}),$$

and if we collect together the sums of equal modulus obtained by replacing x by cx ($c = 1, 2, \dots, p-1$), we deduce

$$\sum_{A_2} \dots \sum_{A_{n_1}} \Big| \sum_x \varepsilon(x) e(x + A_2 x^2 + \dots + A_{n_1} x^{n_1}) \Big|^{2n_1} = O(p^{2n_1 - 1}).$$

Substituting this in (31),

$$\sum_y{}' \Big| \sum_x \varepsilon(x) e(f_y(x)) \Big| = O(p^{1-\frac{1}{2n_1}} p^{1-\frac{1}{2n_1}}) + O(p);$$

hence by (29),

$$S = O(p^{1-\frac{1}{2n_1}}) = \begin{cases} O(p^{\frac{3}{4}}) \text{ if } n = 4 \text{ or } 5, \\ O(p^{\frac{5}{6}}) \text{ if } n = 6 \text{ or } 7. \end{cases}$$

This proves case 1 of the theorem.

Case 2 ($n \geqq 8$). We apply the inequality (30) with r chosen so that the degree $n_r = \left[\frac{n}{2^r}\right]$ of $f_{y_1, \dots, y_r}(x)$ is 2 or 3. There is one and only one such r, and for this r, $2^r n_r$ is the largest number of either of the forms 2^γ, $3 \cdot 2^\gamma$ which does not exceed n. Also $r \geqq 2$. With the notation explained in § 5,

$$|S|^{2^r} \leqq C_r p^{2^r - r - 1} \sum_{j=1}^{2^r} \sum_{y_1}{}' \cdots \sum_{y_r}{}' \Big| \sum_x \varepsilon_j(x; y_3, \dots, y_r)\, e(H_1 x + \dots + H_{n_r} x^{n_r}) \Big| + O(p^{2^r - 1}) .$$

By lemma 2, there are $O(1)$ sets of values of h_1, h_2 for which the congruences (20), (21) have more than $O(1)$ solutions, and for these exceptional values they have $O(p)$ solutions. Hence there are $O(p)$ values of y_1, y_2 which correspond to exceptional values of h_1, h_2. If we exclude these from the summation on the right above, the error made will be

$$O(p^{2^r - r - 1} p^{r-1} p) = O(p^{2^r - 1}) .$$

Hence we can restrict the summation above to be over all other values of y_1, y_2. By Hölder's inequality,

$$\sum_{y_1}{}' \sum_{y_2}{}' \Big| \sum_x \varepsilon_j(x)\, e(H_1 x + \dots + H_{n_r} x^{n_r}) \Big| \leqq p^{2\left(1 - \frac{1}{2n_r}\right)} \Big\{ \sum_{y_1}{}' \sum_{y_2}{}' \Big| \sum_x \varepsilon_j(x)\, e(H_1 x + \dots + H_{n_r} x^{n_r}) \Big|^{2n_r} \Big\}^{\frac{1}{2n_r}}$$

$$= O\Big[p^{2\left(1 - \frac{1}{2n_r}\right)} \Big\{ \sum_{h_1} \sum_{h_2} \cdots \sum_{h_{n_r}} \Big| \sum_x \varepsilon_j(x)\, e(h_1 x + \dots + h_{n_r} x^{n_r}) \Big|^{2n_r} \Big\}^{\frac{1}{2n_r}} \Big] ,$$

since the congruences

$$H_1(y_1, y_2) \equiv h_1 ,$$
$$H_2(y_1, y_2) \equiv h_2 ,$$

have only $O(1)$ solutions in y_1, y_2. Hence by lemma 3,

$$S^{2^r} = O(p^{2^r - r - 1} p^{r-2} p^{2\left(1 - \frac{1}{2n_r}\right)} p^{\frac{2n_r}{2n_r}}) = O(p^{2^r - \frac{1}{n_r}}) ,$$

which is the result ($2^r n_r = m$). This completes the proof of theorem 2.

The sum (5).

8. Theorem 3. *For any fixed n (other than 0),*

$$\sum_x e(ax^n + bx^{2n}) = O(p^{\frac{5}{8}}), \qquad (a \not\equiv 0,\ b \not\equiv 0).$$

Proof: By (10) it suffices to prove that for any Dirichlet character χ,

$$U = \sum_x \chi(x) e(ax + bx^2) = O(p^{\frac{5}{8}}),\ ^1)$$

and we can suppose without loss of generality that χ is not the principal character. We have

$$|U|^2 = \sum_x \sum_y \chi(y)\,\bar{\chi}(x)\, e(ay - ax + by^2 - bx^2)$$

$$= \sum_x{}' \sum_z \chi(z)\, e(ax(z-1) + bx^2(z^2-1)), \tag{32}$$

on writing $y \equiv zx$. The sum over x is a Gaussian sum, and if $z \not\equiv \pm 1$,

$$\sum_x e(ax(z-1) + bx^2(z^2-1)) = \left(\frac{b(z^2-1)}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}\, e\left(-\frac{a^2(z-1)}{4b(z+1)}\right),$$

by the formula quoted in § 3. On substituting in (32), allowing for the terms in which $z \equiv \pm 1$, and writing $\frac{z-1}{z+1} \equiv -x$, we find

$$|U|^2 = p + \varepsilon \sqrt{p}\, V,$$

where $|\varepsilon| = 1$ and

$$V = V(c) = \sum_x \left(\frac{x}{p}\right) \chi(x-1)\,\bar{\chi}(x+1)\, e(cx), \qquad c \equiv \frac{a^2}{4b}.$$

To prove theorem 3 we have to show that $V = O(p^{\frac{3}{4}})$. Applying the transformation (12) to V^2,

$$V^2 = \sum_\xi \sum_\eta \left(\frac{\eta^2 - \xi^2}{p}\right) \chi(\eta^2 - \xi^2 - 2\eta + 1)\,\bar{\chi}(\eta^2 - \xi^2 + 2\eta + 1)\, e(2c\eta)$$

$$= \sum_\eta{}' \sum_x \left(\frac{1-x}{p}\right) \chi\left(x - \left(1 - \frac{1}{\eta}\right)^2\right) \bar{\chi}\left(x - \left(1 + \frac{1}{\eta}\right)^2\right) e(2c\eta)$$

$$+ \sum_\eta{}' \sum_x \left(\frac{x(1-x)}{p}\right) \chi\left(x - \left(1 - \frac{1}{\eta}\right)^2\right) \bar{\chi}\left(x - \left(1 + \frac{1}{\eta}\right)^2\right) e(2c\eta) + O(p),$$

on replacing ξ by ηx in the terms for which $\eta \not\equiv 0$, and using (8). If in the first sum on the right we replace x by

$$\frac{2\eta - 1}{\eta^2} x + 1,$$

and in the second we replace x by

$$\frac{(\eta-1)^2}{-(2\eta-1)x + (\eta-1)^2},$$

the sums over x are expressed in terms of

$$\varphi(m) = \sum_x \left(\frac{x}{p}\right) \chi(x+1)\,\bar{\chi}(x+m),$$

and

$$|V|^2 \leqq \sum_{\eta \not\equiv \frac{1}{2}} \left|\varphi\left(-\frac{2\eta+1}{2\eta-1}\right)\right| + \sum_{\eta \not\equiv \frac{1}{2}, -1} \left|\varphi\left(-\frac{(\eta-1)^2(2\eta+1)}{(\eta+1)^2(2\eta-1)}\right)\right| + O(p)$$

$$\leqq 4 \sum_m |\varphi(m)| + O(p),$$

---

[1]) The implied constant is now an *absolute* constant.

since for given m the congruences

$$-\frac{2\eta+1}{2\eta-1} \equiv m, \quad -\frac{(\eta-1)^2(2\eta+1)}{(\eta+1)^2(2\eta-1)} \equiv m$$

have respectively not more than 1 and 3 solutions in y.

It is known that [1])

$$\sum_m |\varphi(m)|^2 = O(p^2),$$

hence by Cauchy's inequality

$$|V|^2 = O(p^{\frac{1}{2}}p) = O(p^{\frac{3}{2}}),$$

and theorem 3 follows.

The generalised Kloosterman sums.

9. By a *generalised Kloosterman sum* we mean a sum of the form

$$\sum_x{}' \chi(x) e(ax + bx^{-1}),$$

where χ is any Dirichlet character. The original Kloosterman sums are obtained by taking χ to be the principal character χ_0. There is clearly no loss of generality in taking b to be 1, and we therefore introduce the notation

$$S(a) = \sum_x{}' \chi(x) e(ax + x^{-1}) \tag{33}$$

$$S_0(a) = \sum_x{}' e(ax + x^{-1}) \tag{34}$$

for the generalised and original sums respectively.

Lemma 5. *If neither of a, b is congruent to zero,*

$$S(a)\,S(b) = \sum_u{}' \chi(u)\, e((a+b)\,u + u^{-1})\, S(ab\,u^2) + \delta(a,b),$$

where $\delta(a,b) = 0$ if $a \not\equiv b$, and $\delta(a,a) = p\chi(-a^{-1})$.

Proof: In

$$S(a)\,S(b) = \sum_x{}' \sum_y{}' \chi(xy)\, e(ax + by + x^{-1} + y^{-1})$$

make the transformation

$$u \equiv \frac{x}{bxy+1}, \quad v \equiv y(bxy+1), \quad \textit{i. e.,} \quad x \equiv u\,(buv+1), \quad y \equiv \frac{v}{buv+1}.$$

This is a (1, 1) transformation of all x, y for which $bxy \not\equiv -1$ into all u, v for which $buv \not\equiv -1$. Hence

$$\begin{aligned} S(a)\,S(b) = &\sum_{\substack{x \\ bxy \equiv -1}}{}' \sum_y{}' \chi(xy)\, e(ax + by + x^{-1} + y^{-1}) \\ &+ \sum_{\substack{u \\ buv \not\equiv -1}}{}' \sum_v{}' \chi(uv)\, e(au\,(buv+1) + u^{-1} + v^{-1}(buv+1)). \end{aligned}$$

The first double sum on the right is

$$\chi(-b^{-1}) \sum_x{}' e((a-b)x) = \delta(a,b) - \chi(-b^{-1}),$$

and if we complete the second double sum by removing the condition $buv \not\equiv -1$ we must add to compensate

$$-\chi(-b^{-1}) \sum_u{}' e(u^{-1}) = \chi(-b^{-1}).$$

---

[1]) "On the distribution of l'th power residues mod p", Journal Lond. Math. Soc. 7 (1932), lemma 3, p. 120.

Thus

$$S(a)\,S(b) = \sum_u{}' \chi(u)\, e((a+b)u + u^{-1})\, S(abu^2) + \delta(a,b)\,,$$

and the lemma is proved.

Lemma 6. $\sum\limits_w |S(w)|^2 = p^2 - p.$

Proof:

$$\sum_w |S(w)|^2 = \sum_x{}' \sum_y{}' \sum_w \bar{\chi}(x)\chi(y)\, e(wy - wx + y^{-1} - x^{-1}) = p \sum_x{}' 1 = p^2 - p.$$

Theorem 4. *For any* χ,

$$|S(a)| < 2p^{\frac{2}{3}}. \tag{35}$$

Proof: By lemma 5,

$$S^2(a) = \sum_x{}' \chi(x)\, e(2ax + x^{-1})\, S(a^2x^2) + p\chi(-a^{-1}).$$

By another application of lemma 5,

$$\begin{aligned} S^3(a) &= \sum_x{}' \sum_y{}' \chi(xy)\, e(2ax + x^{-1} + (a^2x^2 + a)y + y^{-1})\, S(a^3x^2y^2) \\ &\quad + \sum_x{}' \chi(x)\, e(2ax + x^{-1})\, \delta(a^2x^2, a) + p\chi(-a^{-1})\, S(a) \\ &= \chi(a^{-1}) \sum_x{}' \sum_z{}' \chi(z)\, e(a(1+z)^2 xz^{-1} + (1+z)x^{-1})\, S(az^2) + 3\vartheta p^2, \quad (|\vartheta| \leqq 1), \end{aligned}$$

on writing $axy \equiv z$. Making a linear transformation of x, the sum over x is $S_0(a(1+z)^3z^{-1})$ provided $z \not\equiv -1$. Hence

$$\begin{aligned} |S(a)|^3 &\leqq 4p^2 + \sum_z{}' |S_0(a(1+z)^3z^{-1})\, S(az^2)| \\ &\leqq 4p^2 + \{\sum_z{}' |S_0(a(1+z)^3z^{-1})|^2 \sum_z{}' |S(az^2)|^2\}^{\frac{1}{2}} \\ &\leqq 4p^2 + (3p^2 \cdot 2p^2)^{\frac{1}{2}} < 8p^2, \end{aligned}$$

by lemma 6, on noting that for given w the congruences $a(1+z)^3z^{-1} \equiv w$ and $az^2 \equiv w$ have respectively not more than 3 and 2 solutions in z.

(6) follows from (11) and (35).

10. In this section I outline two other methods of proving that the original Kloosterman sums $S_0(a)$ are $O(p^{\frac{2}{3}})$; these methods do not appear to apply to the generalised sums.

The first method is similar to that just given, but is based on the more elegant multiplication formula

$$S_0(a)\,S_0(b) = \sum_x{}' \left(\frac{x^2 + a^2 + b^2 - 2xa - 2xb - 2ab}{p}\right) S_0(x) + \delta(a,b), \tag{36}$$

where $\delta(a,b)$ is p or 0 according as a, b are or are not congruent. This formula has the advantage of being homogeneous, in the sense that

$$S_0(ka)\,S_0(kb) = \sum_x{}' \left(\frac{x^2 + a^2 + b^2 - 2xa - 2xb - 2ab}{p}\right) S_0(kx) + \delta(a,b).$$

From (36) one deduces that

$$S_0^3(a) = \sum_y \psi(y)\, S_0(ay) + O(p^2)$$

where

$$\psi(y) = \sum_x \left(\frac{(x^2 - 4x)\,(x^2 + y^2 + 1 - 2xy - 2x - 2y)}{p}\right). \tag{37}$$

By a linear fractional transformation $\psi(y)$ can be expressed as

$$\Psi(Y) = \sum_x \left(\frac{x(x^2 + x + Y)}{p}\right)$$

with Y a simple rational function of y. It is immediate that

$$\sum_{Y} \Psi^2(Y) = O(p^2), \tag{38}$$

and by arguments which will now be familiar to the reader it follows that

$$S_0^3(a) = O(p^2).$$

The second method is more direct, though fundamentally equivalent to the previous one. [1]) If

$$S(u, v) = \sum_{x}{}' e(ux + vx^{-1}),$$

we have

$$\sum_{u} \sum_{v} |S(u, v)|^6 = p^2 \sum_{\alpha} \sum_{\beta} \nu^2(\alpha, \beta)$$

where $\nu(\alpha, \beta)$ is the number of solutions of

$$x_1 + x_2 + x_3 \equiv \alpha$$
$$x_1^{-1} + x_2^{-1} + x_3^{-1} \equiv \beta.$$

Evaluating this number in terms of Legendre symbols we find that

$$\nu(\alpha, \beta) = \nu(\alpha\beta, 1) \qquad \text{(unless } \alpha \equiv \beta \equiv 0),$$

and

$$\nu(y, 1) = p + \psi(y) + O(1),$$

where $\psi(y)$ is defined by (37). Using (38),

$$\sum_{u} \sum_{v} |S(u, v)|^6 = p^6 + O(p^5),$$

and on removing the term $|S(0, 0)|^6 = (p-1)^6$ and collecting together the sets of $p-1$ sums of equal modulus,

$$\sum_{a} |S_0(a)|^6 = O(p^4). \tag{39}$$

11. It is well known [2]) that the Kloosterman sums $S_0(a)$ defined by (34) have the alternative expression

$$S_0(a) = \sum_{x} \left(\frac{x^2 - a}{p}\right) e(2x). \tag{40}$$

This is an immediate deduction from the definition, for the number of solutions of $ax + x^{-1} \equiv 2y$ for given y is $1 + \left(\frac{y^2 - a}{p}\right)$, hence

$$\sum_{x}{}' e(ax + x^{-1}) = \sum_{y} e(2y) + \sum_{y} \left(\frac{y^2 - a}{p}\right) e(2y) = \sum_{y} \left(\frac{y^2 - a}{p}\right) e(2y).$$

We shall now show that the generalised Kloosterman sums corresponding to any Dirichlet character χ have a dual expression of the form

$$S(a) = \varepsilon \sum_{x} \chi^*(x^2 - a)\, e(2x),$$

where ε is a factor of unit modulus depending on χ, and χ^* is the product of $\bar{\chi}$ and the Legendre symbol.

Lemma 7. *If χ, χ' are two non-principal characters, not conjugate to one another, then for any λ,*

---

[1]) This is Herr Salié's method.

[2]) Salié, loc. cit. p. 101, equations (51), (52).

$$(41)\quad \sum_x \chi(x)\,\chi'(x-\lambda) = \frac{\tau(\chi')\tau(\bar\chi\bar\chi')}{\tau(\bar\chi)}\,\chi\chi'(\lambda) = \frac{\tau(\chi)\tau(\bar\chi\bar\chi')}{\tau(\bar\chi')}\,\chi\chi'(-\lambda).\ ^{1})$$

Proof: Replacing t by ta in the defiinition of $\tau(\bar\chi)$, we have for any $a \not\equiv 0$,

$$(42)\qquad \chi(a) = \frac{1}{\tau(\bar\chi)} \sum_t \bar\chi(t)\, e(ta)\,,$$

and inspection shows that this is also valid for $a \equiv 0$. Hence

$$\sum_x \chi(x)\,\chi'(x-\lambda) = \frac{1}{\tau(\bar\chi)} \sum_x \sum_t \bar\chi(t)\,\chi'(x-\lambda)\,e(tx) = \frac{1}{\tau(\bar\chi)} \sum_x \sum_t \bar\chi(t)\,e(t\lambda)\,\chi'(x)\,e(tx)$$
$$= \frac{\tau(\chi')}{\tau(\bar\chi)} \sum_t \bar\chi(t)\,\bar\chi'(t)\,e(t\lambda) = \frac{\tau(\chi')\,\tau(\bar\chi\bar\chi')}{\tau(\bar\chi)}\,\chi\chi'(\lambda)\,.$$

The second expression on the right of (41) follows from the first on changing λ into $-\lambda$ and interchanging χ, χ', which leaves the sum on the left unaltered. [2])

Theorem 5. *Let $\chi_1(x)$ denote the Legendre symbol $\left(\frac{x}{p}\right)$. Let $S(a)$ be the generalised Kloosterman sum corresponding to a character χ different from χ_0 and χ_1. Then*

$$(43)\qquad S(a) = \varepsilon(\chi) \sum_x \chi^*(x^2 - a)\, e(2x)\,,$$

where $\chi^* = \bar\chi\chi_1$ and

$$\varepsilon(\chi) = \frac{\tau(\chi\chi_1)}{\tau(\chi_1)}\,\chi(-1)\,.$$

Proof: Substituting from (42) in (33) we have

$$S(a) = \frac{1}{\tau(\bar\chi)} \sum_t \bar\chi(t) \sum_x{}' e(tx + ax + x^{-1})\,.$$

The sum over x is $S_0(t+a)$, hence by (40)

$$S(a) = \frac{1}{\tau(\bar\chi)} \sum_t \bar\chi(t) \sum_x \chi_1(x^2 - (t+a))\, e(2x)\,.$$

By hypothesis χ is different from χ_0 and χ_1, hence we can apply lemma 7 to the summation over t:

$$\sum_t \bar\chi(t)\,\chi_1(t - (x^2 - a)) = \frac{\tau(\bar\chi)\,\tau(\chi\chi_1)}{\tau(\chi_1)}\,\chi^*(-1)\,\chi^*(x^2 - a).$$

Substituting, we obtain the result of the theorem.

It will be seen that we have excluded from the scope of theorem 5 not only the case of the original Kloosterman sums, already dealt with, but also that of the generalised Kloosterman sums formed with the Legendre symbol. But in fact these can be evaluated exactly, and we have [3])

$$(44)\quad \sum_x \left(\frac{x}{p}\right) e(ax + x^{-1}) = \begin{cases} 0 & \text{if} \quad \left(\frac{a}{p}\right) = -1\,, \\ i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}\,(e(2\alpha) + e(-2\alpha)) & \text{if } a \equiv \alpha^2\,. \end{cases}$$

This formula can be used to improve on theorem 4 in the case when χ is a *quartic* character. One can show that in this case

---

[1]) $\tau(\chi) = \sum_t \chi(t)\, e(t)\,, \qquad |\tau(\chi)| = \sqrt{p}\,.$

[2]) It is also a consequence of the well known fact that $\tau(\chi)\,\tau(\bar\chi) = p\,\chi(-1)$.

[3]) Salié, loc. cit. p. 102, equations (54), (57).

(45) $$S(a) = O(p^{\frac{5}{8}}),$$

but the result is hardly of sufficient importance to merit the proof being given here.

12. The sum

$$\sum_x e\left(\frac{ax^2 + 2bx + c}{Ax^2 + 2Bx + C}\right)$$

(in which the zeros of the denominator, if any, are excluded from the summation) is immediately reducible to a Kloosterman sum. For the number of solutions of

$$\frac{ax^2 + 2bx + c}{Ax^2 + 2Bx + C} \equiv y$$

for any given $y \not\equiv \frac{a}{A}$ is

$$1 + \left(\frac{(By - b)^2 - (Ay - a)(Cy - c)}{p}\right),$$

so the sum differs only trivially from

$$\sum_y \left(\frac{(By - b)^2 - (Ay - a)(Cy - c)}{p}\right) e(y);$$

and if we replace y by $y + \frac{2Bb - Ac - Ca}{2(B^2 - AC)}$, this is of the same form as the sum on the right of (40).

Partial Sums.

13. In this section we shall see that the inequalities which have been established for the "complete" exponential sums S_f are also true uniformly in x_1, x_2 for the partial sums

$$S_f(x_1, x_2) = \sum_{x_1}^{x_2} e(f(x)), \qquad (0 \leqq x_1 \leqq x_2 \leqq p),$$

provided that the function $f(x)$ contains a linear term in x. The device by which this extension is made is a familiar one in the analytic theory of numbers.

Lemma 8. *Let $F(x)$ be any function defined for all x mod. p whose absolute value does not exceed some absolute constant, and let*

$$J_s = \sum_x F(x)\, e(sx).$$

Then

$$\left|\sum_{x=1}^{N} F(x) - \frac{N}{p} J_0\right| < \sum_{s=-p+1}^{p-1}{}' \left|\frac{J_s}{s}\right| + O(\log p), \qquad (1 \leqq N < p).$$

Proof: It is well known that if t is not an integer,

$$\{t\} = t - [t] - \tfrac{1}{2} = -\frac{1}{2\pi i} \sum_{s=-p+1}^{p-1}{}' \frac{1}{s}\, e^{2s\pi it} + O\left(\frac{1}{p\,||t||}\right),$$

where $||t||$ denotes the (absolute) difference between t and the nearest integer. Now if x is any integer between 0 and p,

$$\left[\frac{x - \frac{1}{2}}{p}\right] - \left[\frac{x - N - \frac{1}{2}}{p}\right]$$

has the value 1 if $1 \leqq x \leqq N$ and 0 otherwise. Hence

$$\sum_{x=1}^{N} F(x) - \frac{N}{p} J_0 = \sum_x \left(\left\{ \frac{x - N - \frac{1}{2}}{p} \right\} - \left\{ \frac{x - \frac{1}{2}}{p} \right\} \right) F(x)$$
$$= -\frac{1}{2\pi i} \sum_{s=-p+1}^{p-1}{}' \frac{1}{s} \left(e^{-\frac{2s\pi i}{p}\left(N+\frac{1}{2}\right)} - e^{-\frac{s\pi i}{p}} \right) J_s + O\left(\sum_x \frac{1}{p \left\| \frac{x - \frac{1}{2}}{p} \right\|} \right).$$

The last term is $O(\log p)$, and the lemma follows.

Theorem 6. *The inequalities* (3) *and* (4) *are true for the corresponding partial sums as well as as for the complete sums.* (2) *is true for partial sums provided one of the* l*'s is* 1. (6) *is true for partial sums provided* $n = 1$.

Proof: If we take $F(x) = e(f(x))$ in lemma 8, where $f(x)$ is any one of the functions occurring in (3) or (4) or (2) (with one $l = 1$) or (6) (with $n = 1$) and substitute for J_s the known inequality for the complete sum, we obtain an inequality for the partial sum which differs from the one we want by a superfluous factor $\log p$ arising from $\sum_{s=-p+1}^{p-1}{}' \frac{1}{|s|}$. We shall see that in each case this factor can be avoided. For this it is necessary to observe that the methods by which the inequalities for complete sums have been established always permit one to assert not merely that

$$J_s = O(p^\alpha)$$

(with the appropriate α), but also that

$$\sum_s |J_s|^{2k} = O(p^{2k\alpha}) \tag{46}$$

for a certain positive integer k. From this it follows by Hölder's inequality that

$$\left| \sum_{x=1}^{N} e(f(x)) - \frac{N}{p} J_0 \right| < \left(\sum_{s=-p+1}^{p-1}{}' \frac{1}{|s|^{\frac{2k}{2k-1}}} \right)^{\frac{2k-1}{2k}} \left(2 \sum_s |J_s|^{2k} \right)^{\frac{1}{2k}} = O(p^\alpha),$$

and so

$$\sum_{x=1}^{N} e(f(x)) = O(p^\alpha).$$

It remains for us to establish in each of the four cases the existence of an inequality of the form (46).

For (6) with $n = 1$, the required inequality is given by (39). In this case $\alpha = \frac{2}{3}$ and $k = 3$.

For (2) with one of the l's 1, it was proved by Mordell [1]) that

$$\sum_g{}^* |S_g|^{2n} = O(p^{2n-1}), \tag{47}$$

where the summation here is over one from each set of polynomials g which are equivalent in the sense of being transformable into one another by changing x into λx. From this (46) follows a fortiori, with $\alpha = 1 - \frac{1}{2n}$ and $k = n$.

For (3), referring to the proof of theorem 1 and appealing in the last sentence to (47) instead of (2), we have

$$\sum_{a,c} |R(a, c)|^4 = O(p^4),$$

that is,

$$\sum_{a,c} |Q(a, c)|^8 = O(p^6).$$

---

[1]) See loc. cit, equations (14) and (16).

Hence if f is a typical cubic polynomial,

$$\sum_f{}^{**} |S_f|^8 = O(p^5) ,$$

where the summation here is over one from each set of cubic polynomials which are equivalent in the sense of being transformable into one another by changing x into $\lambda x + \mu$. It is easily verified that for any fixed a, b

$$\sum_c |\sum_x e(ax^3 + bx^2 + cx)|^8 < K \sum_f{}^{**} |S_f|^8 ,$$

where K is an absolute constant, and this establishes (46) with $\alpha = \frac{5}{8}$ and $k = 4$.

For (4) we must observe what becomes of the linear term $a_1 x$ in $f(x)$ when we form the first inequality (29) in the proof of theorem 2. It is easily seen that (29) can be written as follows:

$$S^2 = \sum_{y_1}{}' e(2a_1 y_1)\, \theta(y_1) \Big| \sum_x e(f_{y_1}(x)) \Big| + \sum_{y_1}{}' e(2a_1 y_1)\, \theta(y_1) \Big| \sum_x \left(\frac{x}{p}\right) e(f_{y_1}(x)) \Big| + O(p) ,$$

where $\theta(y_1)$ has absolute value 1 and is independent of a_1. From this we have

$$\sum_{a_1} |S_f^2 + O(p)|^2 \leqq 2 \sum_{x_1}{}' \Big| \sum_y e(f_{y_1}(x)) \Big|^2 + 2 \sum_{y_1}{}' \Big| \sum_x \left(\frac{x}{p}\right) e(f_{y_1}(x)) \Big|^2 .$$

Arguing now as in theorem 2 we find

$$\sum_{a_1} |S_f|^4 = O(p^{4-\frac{4}{m}}) ,$$

which is of the form (46) with $\alpha = 1 - \dfrac{1}{m}$ and $k = 2$.

14. Theorem 7. [1]) *If χ is any non-principal Dirichlet character, and $a \not\equiv 0$, $b^2 - 4ac \not\equiv 0$, then*

$$|\sum_{x=x_1}^{x_2} \chi(ax^2 + bx + c)| < K p^{\frac{2}{3}} \log p , \qquad (0 \leqq x_1 \leqq x_2 \leqq p),$$

where K is an absolute constant. Also (a) *if χ is the Legendre symbol,*

$$\left| \sum_{x=x_1}^{x_2} \left(\frac{ax^2 + bx + c}{p}\right) \right| < K p^{\frac{2}{3}};$$

(b) *if χ is a quartic character, other than the Legendre symbol,*

$$|\sum_{x=x_1}^{x_2} \chi(ax^2 + bx + c)| < K p^{\frac{5}{8}} \log p .$$

Proof: We can suppose without loss of generality that $a = 1$, $b = 0$. For convenience replace c by -4λ. By hypothesis $\lambda \not\equiv 0$. Take $F(x) = \chi(x^2 - 4\lambda)$ in lemma 8. Then for $s \not\equiv 0$,

$$J_s = \sum_x \chi(x^2 - 4\lambda)\, e(sx) = \chi\left(\frac{4}{s^2}\right) \sum_x \chi(x^2 - \lambda s^2)\, e(2x) = \theta S(\lambda s^2) ,$$

where S is the generalised Kloosterman sum formed with the character $\chi^* = \bar{\chi}\chi_1$, and $|\theta| = 1$. Also J_0 is easily evaluated by the aid of (42) in terms of various τ's and is found to have absolute value $\sqrt{p}$. Substituting in lemma 8 and using theorem 4,

$$\sum_{x=1}^{N} \chi(x^2 - 4\lambda) = O(\sqrt{p}) + O\left(p^{\frac{2}{3}} \sum_{s=-p+1}^{p-1}{}' \frac{1}{|s|}\right) + O(\log p) = O(p^{\frac{2}{3}} \log p) .$$

For (b), χ^* is a quartic character, and we can use (45) instead of theorem 4. For (a), χ^* is the principal character, and

[1]) This is a generalisation of Pólya's inequality (Landau, Vorlesungen über Zahlentheorie, vol. 2, Satz 194).

$$\sum_{x=1}^{N} \chi(x^2-4\lambda) = O(\sqrt{p}) + O\Big(\sum_{s=-p+1}^{p-1}{}' \Big|\frac{S_0(\lambda s^2)}{s}\Big|\Big) + O(\log p)$$
$$= O\left(\Big\{\sum_{s=-p+1}^{p-1}{}' \frac{1}{|s|^{\frac{6}{5}}}\Big\}^{\frac{5}{6}} \Big\{\sum_{s=-p+1}^{p-1}{}' |S_0(\lambda s^2)|^6\Big\}^{\frac{1}{6}}\right) + O(\sqrt{p})$$
$$= O(\{\sum_a |S_0(a)|^6\}^{\frac{1}{6}}) + O(\sqrt{p}) = O(p^{\frac{2}{3}}),$$

by (39).

Theorem 7 can generalised to polynomials of higher degree, with weaker exponents on the right.

15. We saw in the proof of theorem 7 that if (confining ourselves for simplicity to the original Kloosterman sums)

$$S_0(a) = O(p^\alpha), \qquad (\tfrac{1}{2} \leqq \alpha < 1),$$

for all a, then

$$P(N, a) = \sum_{x=0}^{N}\Big(\frac{x^2-4a}{p}\Big) = O(p^\alpha \log p) \qquad \text{for } a \not\equiv 0,\ 0 \leqq N \leqq p.$$

It may be worth while pointing out an inequality in the opposite direction, namely that if

$$P(N, a) = O(p^\alpha)$$

for $0 \leqq N \leqq p$, then

$$S_0(a) = O(p^\alpha).$$

Thus the orders of magnitude of the Kloosterman sums and of the partial sums $P(N, a)$ differ at most by a factor $\log p$. The proof is immediate, by partial summation:

$$S_0(a) = \sum_{x=0}^{p-1}\Big(\frac{x^2-4a}{p}\Big) e^{\frac{2\pi i x}{p}}$$
$$= (1-e^{\frac{2\pi i}{p}}) \sum_{N=0}^{p-2} P(N, a)\, e^{\frac{2\pi i N}{p}} + P(p-1, a)\, e^{-\frac{2\pi i}{p}}$$
$$= O\Big(\frac{1}{p}\sum_{N=0}^{p-2} |P(N, a)|\Big) + O(|P(p-1, a)|) = O(p^\alpha).$$

Eingegangen 15. Juli 1932.

Zur Differentialgeometrie der Kurven und Flächen.

Von *Otto Haupt* in Erlangen.

Einleitung.

0, 1. Der Gesichtspunkt, unter welchem nachstehend *reelle* Raumkurven und Flächen betrachtet werden sollen, ist derjenige der sogen. „*L-Ordnung*“ (Abkürzung für „lineare Ordnung“). Sie ist für eine Kurve C gleich der maximalen Mächtigkeit des Durchschnittes von C mit einer Ebene, für eine Fläche F gleich der maximalen Mächtigkeit des Durchschnittes mit einer Geraden. Die Fragen, welche sich beim Operieren mit diesem — wie überhaupt mit jedem derartigen — Ordnungsbegriff einstellen, lassen sich zwanglos unterscheiden in Fragen nach dem Verhalten „im Großen“ und in Fragen nach dem Verhalten „im Kleinen“, nach dem Verhalten nämlich der betrachteten Gebilde, hier der Kurven und Flächen.

Im Folgenden soll es sich um eine Frage im Kleinen handeln. Diese Fragestellung werden wir am besten durch Zurückgehen auf den Fall der *ebenen Kurven* erläutern können. Von diesen weiß man [1]): Jede Kurve, welche keine Teilstrecken enthält, ist abgeschlossene Hülle einer Summe von „primitiven“ Bogen, d. h. von Bogen, deren Teilbogen sämtlich die gleiche L-Ordnung besitzen wie der Bogen selbst; und zwar gibt es primitive Bogen nur von den L-Ordnungen zwei und unendlich. Da die Bogen von der L-Ordnung zwei nichts anderes sind als die Konvexbogen, so kann man auch sagen: Jede ebene Kurve verhält sich im Kleinen wesentlich entweder wie ein Konvexbogen oder wie ein primitiver Bogen unendlicher L-Ordnung. Beschränkt man aber die Betrachtung auf *zweimal stetig differenzierbare* Kurven, so fehlen die primitiven Bogen unendlicher L-Ordnung, solche Kurven sind daher abgeschlossene Hüllen von Konvexbogensummen; statt dessen kann man auch sagen: Die konvexen Teilbogen liegen auf solchen Kurven überall dicht.

0, 2. Dieses zuletzt erwähnte Ergebnis soll nun in den folgenden Zeilen auf *Raumkurven* und Flächen verallgemeinert werden. Dem Konvexbogen als einzigem primitiven Element in der Ebene entspricht dann im Falle der Raumkurven, wie wir zeigen, der Bogen dritter L-Ordnung [2]). Wir erhalten infolgedessen den

Satz: Jede im wesentlichen dreimal stetig differenzierbare Raumkurve ist abgeschlossene Hülle einer Summe von Bogen dritter L-Ordnung [3]).

Wir haben dabei immer den Fall ausgeschlossen, daß die betrachtete Raumkurve ebene

---

[1]) Haupt, Über die Struktur reeller Kurven, Crelles Journal 164 (1931), S. 50 ff.

[2]) Jeder Bogen im R_3 (welcher keine ebenen Teilbogen enthält), ist von mindestens dritter L-Ordnung. Und die Bogen dritter L-Ordnung sind zugleich primitiv (von niedrigster L-Ordnung), d. h. jeder Teilbogen eines Bogens dritter L-Ordnung ist selbst von dritter L-Ordnung.

[3]) Vgl. auch Nr. 1, 1.

Teilbogen enthält; bei der Art unserer Fragestellung bedeutet das ersichtlich keinerlei Einschränkung der Allgemeinheit.

0, 3. Im Falle der *Flächen* ist zu vermuten, daß die geradlinigen Flächenstücke [14]) eine Sonderstellung einnehmen, während im übrigen primitive Flächenstücke nur von den Ordnungen zwei und drei möglich sind [4]); in sinngemäßer Übertragung der im Falle der Kurven gebrauchten Bezeichnung nennen wir dabei ein Flächenstück „primitiv" von einer bestimmten L-Ordnung, wenn *jedes* seiner Teilflächenstücke die gleiche L-Ordnung besitzt wie das ursprüngliche Flächenstück. Tatsächlich gilt nun der

Satz: *Jede im wesentlichen dreimal stetig differenzierbare Fläche ist abgeschlossene Hülle einer Summe von primitiven Flächenstücken, deren jedes entweder geradlinig oder von zweiter oder von dritter L-Ordnung ist* [5]).

Wir haben dabei immer den Fall *ausgeschlossen, daß die betrachtete Fläche ebene Teilflächenstücke enthält*; bei der Art unserer Fragestellung bedeutet das ersichtlich keinerlei Einschränkung der Allgemeinheit.

Eine neue Frage ist die nach der Ordnung der primitiven geradlinigen Flächenstücke. Wir gehen auf diese Frage in der vorliegenden Arbeit nicht ein.

0, 4. Die für den dreidimensionalen Raum gewonnenen Ergebnisse übertragen sich fast ohne weiteres auf den Fall des *n-dimensionalen Raumes.* Wir werden dabei *im wesentlichen n-mal stetige Differenzierbarkeit* zu verlangen haben.

An Stelle des Bogens dritter L-Ordnung im Satze über die Raumkurven tritt dann der Bogen n-ter L-Ordnung [6]). Und der Satz über die Flächen im gewöhnlichen Raume R_3 modifiziert sich [7]) für den Fall des R_n dahin, daß an Stelle der im R_3 auftretenden primitiven Flächenstücke zweiter und dritter L-Ordnung als Bausteine im R_n zu treten haben: Primitive Hyperflächenstücke von nicht höherer als n-ter L-Ordnung; hingegen tritt an Stelle der geradlinigen Flächenstücke eine spezielle Klasse von Hyperflächenstücken, welche sich — bis auf eine Realitätsforderung — durch ein System partieller Differentialgleichungen n-ter Ordnung charakterisieren läßt und welche mindestens die geradlinigen Hyperflächenstücke enthält, d. h. diejenigen Hyperflächenstücke, auf welchen durch jeden Punkt eine Gerade geht [7]). Auf diese Klasse, welche bisher, auch vom geometrischen Standpunkt aus, nicht betrachtet zu sein scheint, gehen wir aber hier ebenfalls nicht näher ein.

Ebenso behalten wir uns vor, auf weitere Fragen einzugehen, wie sie sich im R_n für $n \geqq 4$ erheben; also auf die Fragen nach der Struktur hinreichend oft differenzierbarer k-dimensionaler Punktmannigfaltigkeiten des R_n (für $2 \leqq k \leqq n-2$) hinsichtlich ihrer „Ordnung" bezogen auf die Gesamtheit der $(n-k)$-dimensionalen *linearen* Mannigfaltigkeiten des R_n.

Zusatz: Im Sinne der früher entwickelten, allgemeinen Gesichtspunkte [1]) kann das soeben angedeutete Ergebnis formuliert werden wie folgt: Die Menge der Kurven im R_n, welche den erwähnten Differenzierbarkeitsannahmen genügen, enthält primitive Bogen nur von n-ter L-Ordnung. Und entsprechendes gilt für die Hyperflächen des R_n.

Übrigens dürften diese unseren Kurven und Flächen auferlegten Differenzierbarkeitsforderungen in allen Fällen erfüllt sein, welche zunächst für die Anwendung unserer Betrachtungen in Frage kommen.

---

[4]) Jedes Flächenstück im R_3, welches keine Strecken (und keine ebenen Teilflächenstücke) enthält, ist von mindestens zweiter L-Ordnung.

[5]) Genaueres, insbesondere bezüglich des Begriffes der „im wesentlichen dreimal stetig differenzierbaren Fläche", in Nr. 2, 1 ff.

[6]) Vgl. Nr. 1, 3.

[7]) Vgl. Nr. 2, 5.

§ 1. Zerlegungssatz für Kurven.

1, 1. Um den zu beweisenden Zerlegungssatz bequem formulieren zu können, wollen wir vorher den Bereich der zur Betrachtung zugelassenen Bogen festlegen. Unter einem „*im wesentlichen dreimal stetig differenzierbaren*" *Bogen* verstehen wir im folgenden immer ein Streckenbild $x = \varphi(t)$, $y = \psi(t)$, $z = \chi(t)$ von folgender Eigenschaft: x, y, z sollen rechtwinklige, kartesische Koordinaten im dreidimensionalen euklidischen Raume bedeuten. Ferner seien $\varphi(t)$, $\psi(t)$, $\chi(t)$ reelle, eindeutige, stetige Funktionen von t in $0 \leqq t \leqq 1$, welche in ihrem Definitionsbereich *bis auf eine nirgends dichte Menge von Stellen t dreimal stetig differenzierbar* sind; überdies soll der Bogen *keine ebenen Teilbogen* [8]) enthalten, d. h. zu keinem Teilintervall von $0 \leqq t \leqq 1$ sollen vier reelle Zahlen a, b, c, d existieren, so daß $|a| + |b| + |c| > 0$ und $a\varphi(t) + b\psi(t) + c\chi(t) = d$ für alle t des betrachteten Teilintervalles. — Der Begriff des im wesentlichen dreimal stetig differenzierbaren Bogens ist übrigens projektiv invariant.

Unsere Behauptung lautet nunmehr (vgl. Nr. 0, 2):

Satz: Jeder im wesentlichen dreimal stetig differenzierbare Bogen B ist darstellbar als abgeschlossene Hülle einer Summe von höchstens abzählbar vielen Teilbogen der L-Ordnung drei, welche zu je zweien höchstens Endpunkte gemeinsam haben.

Dementsprechend liegen auf B die Punkte höherer als dritter L-Ordnung nirgends dicht; ein *Punkt* P von B heißt dabei „*von der L-Ordnung k*", wenn jede hinreichend kleine Umgebung von P auf B die L-Ordnung k besitzt. Und jeder (im wesentlichen) dreimal stetig differenzierbare primitive Bogen ist von dritter L-Ordnung; dabei heißt ein Bogen „*primitiv*", wenn jeder seiner Punkte bzw. jeder seiner Teilbogen die gleiche Ordnung hat, wie der ganze Bogen.

1, 2. Zum Beweise unseres Satzes ist lediglich zu zeigen [9]): Es gibt keine dreimal stetig differenzierbare Bogen B der Art, daß in *beliebiger* Nähe eines *jeden* Bogenpunktes (mindestens) vier in einer Ebene liegende Bogenpunkte existieren. Daß aber keine solchen Bogen existieren, folgt aus nachstehendem Hilfssatz: Ist $P(t_0)$ ein Punkt von B, in dessen beliebig kleiner Umgebung vier (oder mehr) verschiedene, einer Ebene angehörige Bogenpunkte sich finden, so gilt:

$$(1) \qquad D_3(x, y, z) = \begin{vmatrix} x' & y' & z' \\ x^{(2)} & y^{(2)} & z^{(2)} \\ x^{(3)} & y^{(3)} & z^{(3)} \end{vmatrix}_{t=t_0} = 0.$$

In der Tat: Ist dieser Hilfssatz richtig und würde ein Bogen B nur Punkte der in Rede stehenden Art besitzen, so müßte $D_3(x, y, z)$ identisch Null sein. Mithin wäre B abgeschlossene Hülle einer Summe von ebenen Bogen, gegen die Annahme.

Der Beweis des Hilfssatzes ergibt sich unmittelbar aus dem Schwarz-Stieltjesschen Mittelwertsatze [10]). Seien nämlich P_j $(j = 1, \ldots, 4)$ vier verschiedene, in einer Ebene liegende Bogenpunkte, welche den Parameterwerten t_j entsprechen $(j = 1, \ldots, 4;$ $t_1 < t_2 < t_3 < t_4)$. Dann haben wir:

$$(1) \qquad D_4^*(x, y, z) = \begin{vmatrix} x(t_1) & y(t_1) & z(t_1) & 1 \\ x(t_2) & y(t_2) & z(t_2) & 1 \\ x(t_3) & y(t_3) & z(t_3) & 1 \\ x(t_4) & y(t_4) & z(t_4) & 1 \end{vmatrix} = 0.$$

---

[8]) Unter einem „*Teilbogen*" von $x = \varphi(t)$, usw., $0 \leqq t \leqq 1$, verstehen wir einen durch $x = \varphi(t)$ usw., $t_1 \leqq t \leqq t_2$, definierten Bogen, wo $0 \leqq t_1 < t_2 \leqq 1$ ist.

[9]) Daß dies genügt, ist früher bewiesen worden. Vgl. [1]), a. a. O.

[10]) Vgl. etwa Blaschke, W., Vorlesungen über Differentialgeometrie, 1. Bd., Berlin 1921, § 4.

Andererseits gilt nach dem genannten Mittelwertsatze:

$$D_4^*(x,y,z) = \frac{1}{1!\,2!\,3!}\begin{vmatrix} x(\tau_1) & y(\tau_1) & z(\tau_1) & 1 \\ x'(\tau_2) & y'(\tau_2) & z'(\tau_2) & 0 \\ x^{(2)}(\tau_3) & y^{(2)}(\tau_3) & z^{(2)}(\tau_3) & 0 \\ x^{(3)}(\tau_4) & y^{(3)}(\tau_4) & z^{(3)}(\tau_4) & 0 \end{vmatrix},$$

wobei $\tau_1 = t_1;\ \tau_1 < \tau_2 < t_2;\ \tau_2 < \tau_3 < t_3;\ \tau_3 < \tau_4 < t_4$, also:

$$\begin{vmatrix} x'(\tau_2) & y'(\tau_2) & z'(\tau_2) \\ x^{(2)}(\tau_3) & y^{(2)}(\tau_3) & z^{(2)}(\tau_3) \\ x^{(3)}(\tau_4) & y^{(3)}(\tau_4) & z^{(3)}(\tau_4) \end{vmatrix} = 0\,.$$

Da aber $t_1, \ldots, t_4$ also auch $\tau_2, \ldots, \tau_4$ in beliebiger Nähe von t_0 liegen und da die drei ersten Ableitungen von x, y, z an der Stelle $t = t_0$ stetig sein sollen, so folgt in der Tat (1), w. z. z. w.

1, 3. Die ganze Betrachtung überträgt sich unverändert auf den R_n. Bezeichnen wir als L_n-Ordnung eines Bogens im R_n die maximale Mächtigkeit des Durchschnittes einer Hyperebene [11]) mit dem Bogen, so ist n die minimale L_n-Ordnung eines Bogens ohne hyperebene Teilbogen [11]) und wir haben den

Satz: Auf jedem, bis auf eine nirgends dichte Menge von Stellen des Bogens, n-mal stetig differenzierbaren, von hyperebenen Teilbogen freien, Bogen B des euklidischen R_n liegen die Teilbogen der L_n-Ordnung n überall dicht; d. h. B ist darstellbar als abgeschlossene Hülle einer Summe abzählbar vieler Bogen von minimaler L_n-Ordnung ($n > 3$).

Zufolge des soeben bewiesenen Satzes sind also unter den bis auf eine nirgends dichte Menge von Stellen n-mal stetig differenzierbaren Bogen des R_n die primitiven identisch mit den Bogen der L_n-Ordnung n. Daraus ergibt sich übrigens zugleich die Existenz solcher Bogen.

§ 2. Zerlegungssatz für Flächen.

2, 1. Unter einem „*Flächenstück*" wollen wir, wie stets im folgenden, ein im dreidimensionalen euklidischen Raum R_3 gelegenes, eindeutiges, stetiges Bild der abgeschlossenen Kreisscheibe verstehen. Einem Flächenstück F wird, wie bereits erwähnt, die L-Ordnung n zugeschrieben ($n \geqq 2$), wenn F mit keiner Geraden mehr als n (verschiedene) Punkte gemeinsam hat und mit mindestens einer Geraden auch genau n. Den *Fall, daß F mit einer Geraden ganze Strecken gemeinsam hat*, können wir durch die *Verabredung* einbeziehen, daß eine solche Strecke nur als *ein* Punkt („*verlängerter Punkt*") gezählt wird bei der Bestimmung der L-Ordnung von F; dabei wird man „größte" derartige Strecken zu betrachten haben, d. h. Strecken, die in keiner größeren, auf F und auf der betrachteten Geraden liegenden, Strecke enthalten sind. Dagegen soll *ausgeschlossen* sein, daß F *ebene Teilflächenstücke* [12]) enthält.

Wie bereits aus dem in der Einleitung angegebenen Satze zu entnehmen ist, beschränken wir uns hier auf eine spezielle Gattung von Flächenstücken, die wir kurz als „*im wesentlichen dreimal stetig differenzierbar*" bezeichnen. Wir verstehen darunter solche Flächenstücke, deren jedes darstellbar ist als abgeschlossene Hülle einer Summe von höchstens abzählbar vielen, relativ-einfachen, dreimal stetig differenzierbaren Teil-

[11]) Unter einer „*Hyperebene*" im R_n verstehen wir eine lineare, $(n-1)$-dimensionale Teilmannigfaltigkeit des R_n, unter einem „*hyperebenen Bogen*" im R_n einen Bogen, der ganz in einer Hyperebene des R_n liegt.

[12]) Ist z. B. $z = f(x, y)$, $x^2 + y^2 \leqq 1$, das ursprüngliche Flächenstück, so verstehe man unter einem „*Teilflächenstück*" jedes durch $z = f(x, y)$ definierte Bild eines abgeschlossenen, einfach zusammenhängenden Teilbereiches von $x^2 + y^2 \leqq 1$.

flächenstücken, welche zu je zweien höchstens Randpunkte gemeinsam haben. Dabei heißt ein Flächenstück „*relativ-einfach*", wenn es sich bezüglich eines geeignet gewählten Systems rechtwinkliger kartesischer Koordinaten x, y darstellen läßt vermittelst einer eindeutigen stetigen Funktion $f(x, y)$:

$$z = f(x, y);$$

der Definitionsbereich sei beschränkt, abgeschlossen und einfach zusammenhängend. Und ein solches Flächenstück heißt „dreimal stetig differenzierbar", wenn die partiellen Ableitungen von $f(x, y)$ bis zur dritten Ordnung einschließlich im Innern des Definitionsbereiches existieren und stetig sind. Da es sich bei unserer Fragestellung immer nur um die Untersuchung „im Kleinen" handelt, so bedeutet die in (1) enthaltene Annahme keine wesentliche Beschränkung der Allgemeinheit nachdem schon einmal Differenzierbarkeitsannahmen gemacht werden [13]).

2, 2. Was zunächst die Existenz primitiver, im wesentlichen dreimal stetig differenzierbarer, nicht geradliniger [14]) Flächenstücke anlangt, so sind Beispiele für die L-Ordnungen zwei und drei bekannt.

Beispielsweise ist ein Teilflächenstück der Oberfläche etwa eines Ellipsoids primitiv von der L-Ordnung zwei.

Primitiv von dritter L-Ordnung ist ferner z. B. das Flächenstück F_3, welches definiert ist durch:

$$z = (2 - x)^3 + (y - 2)^3, \text{ etwa im Bereiche } 0 \leqq x \leqq \frac{1}{2}, 0 \leqq y \leqq \frac{1}{3}\, x.$$

In der Tat: Zunächst enthält F_3 keine Strecke [15]). Ist ferner P ein beliebiger Punkt im Innern unseres Flächenstückes F_3 und $\mathfrak{U}(P)$ eine beliebig kleine Umgebung von P, so existiert, wie wir sogleich zeigen werden, eine Gerade g durch P, welche mit $\mathfrak{U}$ außerdem noch 2 verschiedene Punkte aber keine Strecke gemeinsam hat. Da F_3 bzw. $\mathfrak{U}$ höchstens von dritter L-Ordnung sind, so sind sie daher von genau dritter L-Ordnung und F_3 ist als primitiv von dritter L-Ordnung nachgewiesen.

Die gesuchte Gerade g läßt sich konstruieren, wie folgt: Es seien x_0, y_0, z_0 die Koordinaten eines Punktes P im Innern von F_3, also insbesondere $z_0 = (2 - x_0)^3 + (y_0 - 2)^3$. Die Gleichungen von g lauten daher: $x = x_0 + \lambda\xi,\ y = y_0 + \lambda\eta,\ z = z_0 + \lambda\zeta$, wobei $\xi^2 + \eta^2 + \zeta^2 = 1$ und $\zeta \geqq 0$ angenommen werden kann. Die übrigen (von P verschiedenen) Schnittpunkte von g mit F_3 ergeben sich dann vermittelst der Wurzeln λ von

$$[-\xi^3 + \eta^3]\ \lambda^2 + 3\,[a\xi^2 - b\eta^2]\ \lambda + (3[-a^2\,\xi + b^2\,\eta] - \zeta) = 0,$$

---

[13]) In der Tat: Sobald nur angenommen wird, daß die Tangentialebene bis auf eine nirgends dichte Menge von Flächenpunkten existiert und stetig ist, können wir unser Flächenstück darstellen als abgeschlossene Hülle einer Summe von höchstens abzählbar vielen abgeschlossenen Teilflächenstücken mit stetiger Tangentialebene, welche zu je zweien höchstens Randpunkte gemeinsam haben. Jedes solche Teilflächenstück projiziert sich aber in der Umgebung eines jeden Punktes einfach auf eine (geeignet gewählte) Koordinatenebene, läßt sich also sicher als abgeschlossene Hülle einer Summe von Flächenstücken der Gestalt (1) darstellen.

[14]) Ein Flächenstück heißt „*geradlinig*", wenn jeder seiner innern Punkte innerer Punkt (mindestens) einer ganz auf dem Flächenstück gelegenen abgeschlossenen Strecke ist. In diesem Sinne könnte also insbesondere auch jedes *ebene* Flächenstück als geradlinig bezeichnet werden.

[15]) Läge nämlich die Verbindungsstrecke der (von einander verschiedenen) Flächenpunkte $P(x', y', z')$ und $Q(x'', y'', z'')$ ganz auf der Fläche und setzt man $x'' - x' = \xi,\ y'' - y' = \eta,\ z'' - z' = \zeta$, so müßte z. B. $z' + \lambda\zeta = (2 - x' - \lambda\xi)^3 + (y' + \lambda\eta - 2)^3$ identisch in λ sein. Dann wäre aber $-\xi^3 + \eta^3 = 0$, also $\xi = \eta$ und folglich $3[(2 - x') + (y' - 2)]\xi^2 = 0$. *Entweder* wäre daher $x' = y'$, mithin auch $x'' = y''$, entgegen den Annahmen über den Definitionsbereich *oder* es wäre $\xi = 0$ und folglich $\eta = 0$, also $x' = x''$, $y' = y''$ und $z' = z''$ im Widerspruch zu der Annahme $P \neq Q$.

wobei $a = 2 - x_0$ und $b = 2 - y_0$ beide positiv sind. Wir haben zu zeigen: Durch passende Wahl von ξ und η (im Rahmen der Bedingung $\xi^2 + \eta^2 = 1 - \zeta^2 \leqq 1$) kann erreicht werden, daß genau zwei, untereinander und von Null verschiedene reelle Wurzeln λ existieren, welche ihrem absoluten Betrage nach beliebig klein sind, daß also unsere Gerade, außer P, noch zwei, zu P beliebig benachbarte, Punkte mit F_3 gemeinsam hat. Um dies zu erreichen, setzen wir: $A = {}_+\sqrt{a}$, $B = {}_+\sqrt{b}$ und $\xi = -\sigma B$, $\eta = \sigma A$. Dann hat in der obigen Gleichung der Koeffizient von λ den Wert Null und die noch verfügbare reelle Konstante σ braucht nur so gewählt zu werden, daß

$$[\zeta + 3\,(a^2\,\xi - b^2\eta)] : [\eta^3 - \xi^3] = [{}_+\sqrt{1 - \sigma^2(a+b)} - 3\sigma\,(a^2\,B + b^2\,A)] : [\sigma^3\,(A^3 + B^3)]$$

positiv und beliebig klein, hingegen $1 - \sigma^2(a+b)$ nicht negativ ausfällt. Das Gewünschte wird aber geleistet von jedem $\sigma = \sigma_0 - \varepsilon$, wobei

$$\sigma_0 = 1 : {}_+\sqrt{a + b + 9\,(a^2\,B + b^2\,A)^2}$$

gesetzt und $\varepsilon > 0$ beliebig — aber hinreichend — klein gewählt ist.

2, 3. Nachdem in Nr. 2, 2 die Existenz (im wesentlichen) dreimal stetig differenzierbarer und nicht geradliniger [14]), primitiver Flächenstücke der L-Ordnungen zwei und drei festgestellt ist, soll jetzt gezeigt werden:

Primitive, im wesentlichen dreimal stetig differenzierbare Flächenstücke, welche keine geradlinigen Teilflächenstücke enthalten, besitzen höchstens die L-Ordnung drei.

Beweis: Ersichtlich kann die Betrachtung beschränkt werden auf Flächenstücke, welche relativ-einfach und dreimal stetig differenzierbar sind. Es sei also $z = f(x, y)$ das gegebene Flächenstück und $f(x, y)$ dreimal stetig differenzierbar, etwa in $x^2 + y^2 < 1$. Es seien ferner $P_\nu\{x_\nu, y_\nu, z_\nu\}$, $\nu = 1, \ldots, 4$, vier verschiedene, auf einer Geraden g gelegene Flächenpunkte. Wir denken uns g orientiert und die P_ν von vorneherein so numeriert, daß P_1 auf g unterhalb P_2, dieses unterhalb P_3 und letzteres unterhalb P_4 liegt, oder, wie wir sagen wollen, daß $P_1, \ldots, P_4$ auf g „*natürlich angeordnet*“ sind.

Da g nicht zur z-Achse parallel sein kann, so gibt es drei reelle, nur von g abhängige Zahlen a, b, c mit $a^2 + b^2 = 1$, so daß für irgend zwei verschiedene Punkte $\bar{P}(\bar{x}, \bar{y}, \bar{z})$ und $P^*\,(x^*, y^*, z^*)$ auf g gilt:

$$(R) \qquad \bar{x} - x^* = t \cdot a, \quad \bar{y} - y^* = t \cdot b, \quad \bar{z} - z^* = t \cdot c;$$

dabei bezeichnet t eine, von Null verschiedene, von $\bar{P}$, P^* abhängige, reelle Zahl.

Aus $z_\nu = f(x_\nu, y_\nu) = F(P_\nu)$, $\nu = 1, \ldots, 4$, folgt nun, vermöge des Mittelwertsatzes:

$$z_\nu - z_\mu = F'_x\,(P_{\nu\mu})\,(x_\nu - x_\mu) + F'_y\,(P_{\nu\mu})\,(y_\nu - y_\mu)\,,$$

also wegen (R)

$$(1) \qquad c = F'_x(P_{\nu\mu})\,a + F'_y(P_{\nu\mu})b, \qquad \nu < \mu;\ \nu, \mu = 1, 2, 3, 4;$$

dabei bezeichnet $P_{\nu\mu}$ einen geeignet gewählten Punkt auf g zwischen P_ν und P_μ.

Entsprechend ergibt sich aus (1):

$$(2') \quad 0 = F^{(2)}_{xx}\,(P_{\tau\nu\mu})a^2 + 2F^{(2)}_{xy}\,(P_{\tau\nu\mu})\,ab + F^{(2)}_{yy}(P_{\tau\nu\mu})\,b^2;\ \tau, \nu, \mu = 1, \ldots, 4,$$

wobei etwa $\tau < \nu < \mu$ und wobei $P_{\tau\nu\mu}$ einen geeignet gewählten Punkt zwischen $P_{\tau\nu}$ und $P_{\nu\mu}$ bezeichnet. Schließlich folgt aus (2') ebenso:

$$(3') \quad 0 = F^{(3)}_{xxx}\,(P_{1234})\,a^3 + 3F^{(3)}_{xxy}(P_{1234})\,a^2\,b + 3F^{(3)}_{xyy}\,(P_{1234})\,ab^2 + F^{(3)}_{yyy}\,(P_{1234})\,b^3;$$

und dabei bezeichnet P_{1234} einen geeigneten Punkt auf g zwischen P_{123} und P_{234}.

Soll nun das vorgelegte Flächenstück primitiv von mindestens vierter L-Ordnung sein, so gibt es Punktquadrupel $P_1, \ldots, P_4$ der oben betrachteten Art in beliebiger Nähe eines jeden (vorgegebenen) Punktes P_0 des Flächenstückes. Wir können also eine Folge von solchen (je auf einer Geraden liegenden) Punktquadrupeln $\mathfrak{Q}_\nu$, $\nu = 1, 2, \ldots$, konstruieren, welche gegen $P_0(x_0, y_0, z_0)$ konvergieren. Sind a_ν, b_ν die zu $\mathfrak{Q}_\nu$ gehörigen a, b, so existiert wegen $|a_\nu| \leqq 1, |b_\nu| \leqq 1$ eine Teilfolge $\mathfrak{Q}_{\nu_\varrho}$, für welche gleichzeitig $\lim\limits_{\varrho\to\infty} a_{\nu_\varrho} = a_0$ und $\lim\limits_{\varrho\to\infty} b_\nu = b_0$ existiert (mit $a_0^2 + b_0^2 = 1$). Da außerdem $f(x, y)$ in der Umgebung von P_0 dreimal stetig differenzierbar sein soll, so ergibt der Grenzübergang in (2′) und (3′): Zu *jedem* Punkte $P_0(x_0, y_0, z_0)$ des primitiven Flächenstückes gehört mindestens ein Paar reeller Zahlen a_0, b_0 mit $a_0^2 + b_0^2 = 1$, so daß gleichzeitig

$$f_{xx}^{(2)}(x_0, y_0)\, a_0^2 + 2 f_{xy}^{(2)}(x_0, y_0)\, a_0 b_0 + f_{yy}^{(2)}(x_0, y_0)\, b_0^2 = 0 \tag{2}$$

$$f_{xxx}^{(3)}(x_0, y_0)\, a_0^3 + 3 f_{xxy}^{(3)}(x_0, y_0)\, a_0^2 b_0 + \cdots + f_{yyy}^{(3)}(x_0, y_0)\, b_0^3 = 0. \tag{3}$$

Aus (2) folgt zunächst, daß die Diskriminante $D = (f_{xy}^{(2)})^2 - f_{xx}^{(2)} f_{yy}^{(2)}$ nirgends negativ ist. *Sehen wir von abwickelbaren Flächenstücken — als einem Sonderfall der geradlinigen — ab*, so kann ohne Beschränkung der Allgemeinheit angenommen werden, daß D positiv ist im Innern des ganzen Flächenstückes; denn wegen der Stetigkeit der zweiten Ableitungen ist die Diskriminante entweder überall Null oder in einem (ebenfalls primitiven) Teilflächenstück (von der gleichen L-Ordnung) durchaus positiv. In jedem (inneren) Punkte unseres Flächenstückes gibt es dann zwei reelle verschiedene Haupttangenten. Wegen der vorausgesetzten dreimal stetigen Differenzierbarkeit können wir die (reellen) Haupttangentenkurven auf unserem Flächenstück in der Umgebung eines Punktes P^* darstellen durch zwei Funktionenpaare:

$$x = \chi_1(t; t_0, x_0, y_0), \quad y = \varphi_1(t; t_0, x_0, y_0) \quad \text{und} \quad x = \chi_2(t; t_0, x_0, y_0), \; y = \varphi_2(t; t_0, x_0, y_0),$$

welche nach t zweimal differenzierbar sind [16]), den Anfangsbedingungen:

$$x_0 = \chi_1(t_0; t_0, x_0, y_0), \quad y_0 = \varphi_1(t_0; t_0, x_0, y_0)$$

usw. genügen, während die ersten Ableitungen $\frac{d\chi_1}{dt}, \frac{d\varphi_1}{dt}$ $\left(\text{bzw. } \frac{d\chi_2}{dt}, \frac{d\varphi_2}{dt}\right)$ niemals beide gleichzeitig Null werden und stetige Funktionen von t, t_0, x_0, y_0 sind [17]). Wir können infolgedessen in (2) und (3) statt a_0, b_0 auch setzen

$$\text{entweder } \left(\frac{d\chi_1}{dt}\right)_{t=t_0}, \left(\frac{d\varphi_1}{dt}\right)_{t=t_0} \text{ oder } \left(\frac{d\chi_2}{dt}\right)_{t=t_0}, \left(\frac{d\varphi_2}{dt}\right)_{t=t_0}.$$

Ohne Beschränkung der Allgemeinheit können wir jetzt unser (primitives) *Flächenstück* (in der Umgebung von P^*) *so gewählt denken, daß in* (2) *und* (3) *ausnahmslos* a_0 *durch* $\left(\frac{d\chi_1}{dt}\right)_{t=t_0}$ *und* b_0 *durch* $\left(\frac{d\varphi_1}{dt}\right)_{t=t_0}$ *ersetzt werden darf.* In der Tat: Bezeichnet M_1 bzw. M_2 die Menge der Punkte P_0 unseres Flächenstückes, für welche $\left(\frac{d\chi_1}{dt}\right)$ bzw. $\left(\frac{d\chi_2}{dt}\right)$ an Stelle von a_0 zu setzen ist [18]), so muß mindestens eine dieser beiden Mengen, etwa M_1, auf mindestens

---

[16]) Die zweimalige Differenzierbarkeit von $x = \chi_1(t)$ usw., nach t folgt daraus, daß χ_1, usw., als Lösung eines Differentialgleichungensystems von folgender Gestalt definiert werden kann: $\frac{dx}{dt} = g(x, y)$, $\frac{dy}{dt} = h(x, y)$, wo also die rechten Seiten (stetig) differenzierbare Funktionen nur von x und y sind.

[17]) Vgl. z. B. Kamke, E., Differentialgleichungen reeller Funktionen, Leipzig 1930, Seite 161, Satz 2.

[18]) Der Durchschnitt von M_1 und M_2 braucht nicht als leer angenommen zu werden.

einem (ebenfalls primitiven) Teilflächenstück, etwa auf $\bar{F}$, dicht sein, da das ganze Flächenstück Vereinigung von M_1 und M_2 ist. Nun sind aber M_1 sowohl als M_2 abgeschlossen, wie aus den Stetigkeitseigenschaften von $f^{(2)}_{xx}$, $f^{(3)}_{xxx}$ usw. und von $\left(\frac{d\chi_1}{dt}\right)_{t=t_0}$ usw. als Funktionen von x_0, y_0 hervorgeht. Daher enthält M_1 das ganze Flächenstück $\bar{F}$, woraus die Zulässigkeit unserer Annahme folgt.

Setzen wir alsdann $\chi = \chi_1(t; x_0, y_0)$, $\varphi = \varphi_1(t; x_0, y_0)$, ferner $\chi' = \frac{d\chi}{dt}$, $\varphi' = \frac{d\varphi}{dt}$, bei irgendwie gegebenem x_0, y_0, so gilt identisch in t

$$(2^*) \qquad f^{(2)}_{xx}(\chi, \varphi)\,(\chi')^2 + 2\,f^{(2)}_{xy}(\chi, \varphi)\,\chi'\,\varphi' + f^{(2)}_{yy}(\chi, \varphi)\,(\varphi')^2 = 0$$

$$(3^*) \quad f^{(3)}_{xxx}(\chi, \varphi)\,(\chi')^3 + 3f^{(3)}_{xxy}(\chi, \varphi)\,\chi'^2\,\varphi' + \cdots + f^{(3)}_{yyy}(\chi, \varphi)\,(\varphi')^3 = 0.$$

Nun ist aber (2*) differenzierbar als Funktion von t, weil sowohl $f^{(2)}_{xx}$ usw., als auch χ', φ' differenzierbar sind. Daher erhalten wir unter Berücksichtigung von (3*)

$$(2^{**}) \quad f^{(2)}_{xx}(\chi, \varphi)\,\chi'\,\chi^{(2)} + f^{(2)}_{xy}(\chi, \varphi)\,[\chi^{(2)}\,\varphi' + \chi'\,\varphi^{(2)}] + f^{(2)}_{yy}(\chi, \varphi)\;\varphi'\,\varphi^{(2)} = 0.$$

Faßt man (2**) und (3*) als lineare homogene Gleichungen in $f^{(2)}_{xx}\,\chi' + f^{(2)}_{xy}\,\varphi'$ und $f^{(2)}_{xy}\,\chi' + f^{(2)}_{yy}\,\varphi'$ auf, so ist — für geeignet gewählte Teilflächenstücke — identisch in t *entweder* $f^{(2)}_{xx}\,\chi' + f^{(2)}_{xy}\,\varphi' = 0$ und $f^{(2)}_{xy}\,\chi' + f^{(2)}_{yy}\,\varphi' = 0$ *oder* $\chi'\,\varphi^{(2)} - \chi^{(2)}\,\varphi' = 0$. Da $(\chi')^2 + (\varphi')^2 > 0$, so ist der erstere Fall wegen $D > 0$ unmöglich. Somit gilt: $\chi^{(2)}(t) = \varrho(t)\,\chi'(t)$ und $\varphi^{(2)}(t) = \varrho(t)\,\varphi'(t)$, folglich $\varphi(t) = c\chi(t) + d$ bzw. $\chi(t) = c\varphi(t) + d$, wo c und d Konstante bedeuten (die nur von x_0, y_0 abhängen). *Die Haupttangentenkurven der einen Schar liegen somit in Lotebenen zur x, y-Ebene.* Nimmt man eine hinreichend kleine Drehung des Koordinatensystems etwa um die x-Achse vor, so wird in der Umgebung eines geeignet gewählten Punktes unseres Flächenstückes letzteres wiederum die Darstellung $\tilde{z} = \Phi(\tilde{x}, \tilde{y})$ mit dreimal stetig differenzierbarem Φ gestatten. Wiederholung aller unserer Schlüsse zeigt dann, daß die Haupttangentenkurven mindestens einer Schar in Ebenen liegen, welche mindestens zwei verschiedenen Parallelebenenbüscheln angehören, daß sie also Gerade sind gegen die Voraussetzung [19]).

2, 4. Mittelst der in Nr. 2, 3 gewonnenen Ergebnisse folgt jetzt leicht der in Nr. 0,3 angekündigte Satz. Man braucht nur den allgemeinen Zerlegungssatz [1]) auf den vorliegenden Fall anzuwenden. Wir erhalten so den

Satz: Jedes Flächenstück, welches im wesentlichen dreimal stetig differenzierbar ist und keine ebenen Teilflächenstücke enthält, kann dargestellt werden als abgeschlossene Hülle einer Summe von primitiven Flächenstücken, welche zu je zweien höchstens Randpunkte gemeinsam haben und deren jedes entweder geradlinig [14]) oder von zweiter oder von dritter L-Ordnung ist.

2, 5. Die bisherigen, für den Fall des R_3 angestellten Überlegungen übertragen sich zum Teil unmittelbar auf den Fall des R_n ($n \geqq 4$): Man erklärt zunächst den Begriff des „*Hyperflächenstückes*“ im R_n und ebenso den Begriff der „*im wesentlichen n-mal stetigen Differenzierbarkeit*“ (vgl. Nr. 2, 1). Sodann zeigt man (ganz entsprechend wie in Nr. 2, 3), daß primitive, im wesentlichen n-mal stetig differenzierbare Hyperflächenstücke

---

[19]) Die gleichzeitige Gültigkeit von (2*) und (3*) als *notwendige* Bedingung dafür, daß das betrachtete Flächenstück geradlinig ist, findet sich z. B. bei Serret-Scheffers, Lehrbuch der Differential- und Integralrechnung, 8. Auflage, 1. Bd., Leipzig 1924, Seite 561/62. — Nachdem festgestellt ist, daß die Haupttangentenkurven der einen Schar eben sind, könnte man auch so weiterschließen: Da unser Flächenstück nicht geradlinig sein soll, so müßte seine Krümmung längs der ebenen Haupttangentenkurven Null sein (Satz von Enneper, vgl. Blaschke [10]), a. a. O., Seite 76), während sie doch als negativ vorausgesetzt war.

im R_n höchstens die Ordnung n besitzen, falls sie keine Teilflächenstücke enthalten, welche der folgenden Bedingung genügen: Ist

$$x_n = f(x_1, \ldots, x_{n-1})$$

die Gleichung des betrachteten Teilflächenstückes, so gibt es zu jedem seiner Punkte $x_1^{(0)}, \ldots, x_{n-1}^{(0)}$ ein System *reeller* Zahlen $a_1^{(0)}, \ldots, a_{n-1}^{(0)}$, welche nicht sämtlich Null sind und den (homogenen) Gleichungen genügen:

$$(\tau') \qquad \Phi_\tau(a_1, \ldots, a_{n-1}) = \Big(\sum_{\nu=1}^{n-1} \frac{\partial}{\partial x_\nu} a_\nu^{(0)}\Big)^{(\tau)} (f) = 0, \quad x_\nu = x_\nu^{(0)}, \qquad \tau = 2, \ldots, n.$$

Sehen wir von der Forderung der Realität der $a_1, \ldots, a_{n-1}$ ab, so ist für das Bestehen von (τ') notwendig und hinreichend, daß das Resultantensystem der Formen $\Phi_\tau(a_1, \ldots, a_{n-1})$ identisch in $x_1, \ldots, x_{n-1}$ verschwindet; für die Berechnung des Resultantensystems sind dabei die Φ_τ als Formen in den Unbestimmten $a_1, \ldots, a_{n-1}$ aufzufassen und ihre Koeffizienten ebenfalls als Unbestimmte zu nehmen, für welche letztere hinterher die betreffenden partiellen Ableitungen von f nach $x_1, \ldots, x_{n-1}$ eingesetzt werden [20]). Das Verschwinden des Resultantensystems ist aber gleichbedeutend mit gewissen algebraischen Relationen, welche für die partiellen Ableitungen von $f(x_1, \ldots, x_{n-1})$ bis zur n-ten Ordnung einschließlich erfüllt sein müssen. Unter den in Rede stehenden Flächenstücken sind die geradlinigen enthalten. Denkt man sich ein solches etwa in der Form dargestellt: $x_n = h(x_1, \ldots, x_{n-2}) + x_{n-1}\, g(x_1, \ldots, x_{n-2})$, so sind für

$$f(x_1, \ldots, x_{n-1}) = h(x_1, \ldots, x_{n-1}) + x_{n-1}\, g(x_1, \ldots, x_{n-2})$$

in der Tat die Bedingungen (τ') identisch erfüllt, wenn man $a_1 = \cdots = a_{n-2} = 0$, $a_{n-1} = 1$ setzt.

---

[20]) Vgl. z. B. Perron, O., Algebra, 1. Bd., 2. Aufl., Berlin 1932,; van der Waerden, B. L., Moderne Algebra, 2. Teil, Berlin 1931, § 76.

Eingegangen 9. Juni 1932.

Über einen Satz von Laguerre.

Von *Julius v. Sz. Nagy* in Szeged (Ungarn).

1. Einleitung.

Von E. Laguerre rührt der folgende Satz her [1]):

Ist $f(x)$ ein Polynom höchstens n-ten Grades und ist ξ eine beliebige Stelle der komplexen x-Ebene, für die $f(\xi) \cdot f'(\xi) \neq 0$ ist, so liegt im Innern oder am Rande eines jeden Kreises durch die beiden Punkte ξ und $\xi - n \frac{f(\xi)}{f'(\xi)}$ mindestens eine Nullstelle von $f(x)$. Liegen nicht alle Nullstellen von $f(x)$ auf dem Rande eines solchen Kreises, so gehören auch seinem Äußeren Nullstellen von $f(x)$ an.

Eine Verschärfung dieses Satzes ist der folgende Satz von L. Fejér [2]):

Ist $f(\xi) \cdot f'(\xi) \neq 0$ und ist p die Anzahl derjenigen Glieder der Folge $f'(\xi), f''(\xi), \ldots, f^{(n)}(\xi)$, die nicht verschwinden, so hat das Polynom $f(x)$ n-ten Grades mindestens eine Nullstelle im Innern oder am Rande eines jeden Kreises durch die beiden Punkte ξ und $\xi - p \frac{f(\xi)}{f'(\xi)}$.

Der Fejérsche Satz besagt nur in jenen endlichvielen Punkten ξ der x-Ebene mehr, als der Laguerresche Satz, wo mindestens eine der Ableitungen des Polynoms $f(x)$ n-ten Grades: $f''(x)$, $f'''(x)$, . . ., $f^{(n)}(x)$ verschwindet.

Wir werden die folgende Verschärfung des Laguerreschen Satzes beweisen:

I. *Es sei $f(x)$ ein Polynom, es sei ξ eine beliebige Stelle der x-Ebene, für die $f(\xi) \cdot f'(\xi) \neq 0$ ist, und es sei g eine beliebige Gerade durch den Punkt ξ. Enthält nun die den Punkt $\xi - \frac{f(\xi)}{f'(\xi)}$ enthaltende und von g berandete Halbebene höchstens p Nullstellen von $f(x)$ in ihrem Inneren, so liegt mindestens eine Nullstelle im Innern oder am Rande des Kreises, der durch die beiden Punkte ξ und $\xi - p \frac{f(\xi)}{f'(\xi)}$ hindurchgeht und im Punkte ξ die Tangente g hat. Enthält der Rand dieses Kreises alle Nullstellen von $f(x)$, die im Innern der angenommenen Halbebene liegen, so hat das Polynom p Nullstellen auf dem Rande des Kreises, die übrigen Nullstellen von $f(x)$ liegen alle auf der Geraden g.*

Dieser Satz enthält den Satz von Laguerre, er sagt aber unter gewissen Umständen mehr aus. Es gilt nämlich der folgende Satz:

II. *Ist ξ eine beliebige Stelle im Innern oder am Rande des kleinsten konvexen Polygons, das sich um die Nullstellen des Polynoms $f(x)$ n-ten Grades spannen läßt und ist $f(\xi) \cdot f'(\xi) \neq 0$, so hat das Polynom im Innern oder am Rande eines jeden Kreises durch die beiden Punkte ξ und $\xi - (n-1) \frac{f(\xi)}{f'(\xi)}$ mindestens eine Nullstelle.*

---

[1]) Nouvelles Annales de math. (2) **17** (1878), Oeuvres de Laguerre I, S. 56—63.

[2]) Jahresbericht d. DMV. **26** (1917), S. 114—128, insbesondere S. 124.

Eine Gerade g durch einen solchen Punkt ξ teilt nämlich die Ebene in zwei Halbebenen, von denen keine mehr als n-1 Nullstellen von $f(x)$ im Innern enthalten kann.

Außerdem werden wir für die Lage der Nullstellen des Polynoms $f(x)$ noch weitere analoge Sätze beweisen, in denen die Rolle der Funktion $\frac{f'(x)}{f(x)}$ ihre höheren Ableitungen, und die Rolle der Kreise Sinusspiralen von ganzem positiven Index übernehmen.

Durch Anwendung dieser Sätze auf die Gleichungen von der Form

$$(1) \qquad f(x) = 1 - x^q + a_{q+1}\, x^{q+1} + a_{q+2}\, x^{q+2} + \cdots + a_n\, x^n = 0 \quad (q \geqq 2)$$

erhalten wir Sätze, die mit einem anderen Satze von L. Fejér im Zusammenhange stehen[3]). Unsere so erhaltenen Sätze bestimmen ein Gebiet der komplexen Ebene, das mindestens eine Wurzel der Gleichung (1) enthält und das im allgemeinen kleiner ist, als der durch den Satz von L. Fejér bestimmte Kreis.

2. Beweis des Laguerreschen Satzes und seiner Verschärfung.

Bezeichnen $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Nullstellen des Polynoms $f(x)$ n-ten Grades, so besteht die Gleichung

$$(2) \qquad -\frac{f'(\xi)}{f(\xi)} = \frac{1}{\alpha_1 - \xi} + \frac{1}{\alpha_2 - \xi} + \cdots + \frac{1}{\alpha_n - \xi}$$

Sind $\alpha_h - \xi = r_h\, e^{i\varphi_h} = r_h\, e^{i(\varphi_h + \omega)}$ und $-\frac{f(\xi)}{f'(\xi)} = R\, e^{i\psi} = R\, e^{i(\psi+\omega)}$ $(h = 1, 2, \ldots, n)$, wo ω einen beliebigen Winkel bezeichnet, für den die Ungleichung $\cos\varphi = \cos(\psi - \omega) > 0$ besteht, so gilt für den reellen Teil der Gleichung

$$-e^{i\omega}\frac{f'(\xi)}{f(\xi)} = e^{i\omega}\left[\frac{1}{\alpha_1 - \xi} + \frac{1}{\alpha_2 - \xi} + \cdots + \frac{1}{\alpha_n - \xi}\right]$$

die Gleichung

$$(3) \qquad \frac{\cos\varphi}{R} = \frac{\cos\varphi_1}{r_1} + \frac{\cos\varphi_2}{r_2} + \cdots + \frac{\cos\varphi_n}{r_n}.$$

Bezeichnet f bzw. g die Gerade, die durch den Punkt ξ hindurchgeht und mit der reellen Achse den Winkel ω bzw. $\omega + \frac{\pi}{2}$ bildet, so ist $\frac{\cos\varphi_h}{r_h}$ positiv oder negativ, je nachdem der Punkt α_h auf derselben bzw. auf der anderen Seite der Geraden g liegt, wie der Punkt $\xi - \frac{f(\xi)}{f'(\xi)}$. Liegt der Punkt α_h auf der Geraden g, so verschwindet das entsprechende Glied der Gleichung (3).

Wir nehmen an, daß die Indizes der Nullstellen von $f(x)$ so gewählt sind, daß die ersten p Glieder der rechten Seite in der Gleichung (3) positiv, die folgenden q Glieder negativ und die letzten n-p-q Glieder Null sind, und daß die Relationen

$$\frac{\cos\varphi_1}{r_1} \geqq \frac{\cos\varphi_2}{r_2} \geqq \cdots \geqq \frac{\cos\varphi_p}{r_p}, \qquad \frac{-\cos\varphi_{p+1}}{r_{p+1}} \geqq \frac{-\cos\varphi_{p+2}}{r_{p+2}} \geqq \cdots \geqq \frac{-\cos\varphi_{p+q}}{r_{p+q}}$$

bestehen. Sind

$$(4) \qquad A = \frac{R}{\cos\varphi}, \quad a_h = \frac{r_h}{\cos\varphi_h}\ (h = 1, 2, \ldots, p), \quad b_k = -\frac{r_{p+k}}{\cos\varphi_{p+k}}\ (k = 1, 2, \ldots, q),$$

so läßt sich die Gleichung (3) in der Form

[3]) A. a. O. und außerdem Comptes Rendus **145** (1907), S. 459, Math. Annalen **65** (1908), S. 413—423. Vgl. auch P. Montel, Ann. de l' École Norm. Sup. (3) **40** (1923), S. 1—34; E. B. Van Vleck, Bull. de la Soc. Math., **53** (1925), S. 105—125; M. Biernacki, Bull. de l'Acad. Pol. d. Sc. et d. Lettr., Cl. d. Sc. Math. et Natur. Série A: Sc. Math. 1927, S. 541—685.

$$\frac{1}{A} = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_p} - \frac{1}{b_1} - \frac{1}{b_2} - \cdots - \frac{1}{b_q} \tag{5}$$

schreiben, wo $0 < A$, $0 < a_1 \leqq a_2 \leqq \cdots \leqq a_p$, $0 < b_1 \leqq b_2 \leqq \cdots \leqq b_q$ sind.

Hier bedeutet a_h bzw. b_h den Durchmesser des Kreises, der durch die beiden Punkte ξ und α_h bzw. α_{p+h} hindurchgeht und im Punkte ξ die Gerade g berührt.

Aus der Gleichung (5) folgt die Ungleichung

$$\frac{p}{a_1} \geqq \frac{1}{A} \quad \text{oder} \quad a_1 \leqq pA (\leqq n A), \tag{6}$$

wo das Gleichheitszeichen nur dann bestehen kann, wenn $a_1 = a_2 = \cdots = a_p$ und $q = 0$ ist. Durch diese Ungleichung sind die Sätze I und II bewiesen.

Aus der Gleichung (5) folgen auch die Ungleichungen

$$\frac{p}{a_1} \geqq \frac{1}{A} + \frac{q}{b_q}, \qquad \frac{1}{a_1} \leqq \frac{1}{A} + \frac{q}{b_1}$$

die sich in Sätzen leicht ausdrücken lassen [4]).

3. Die Verallgemeinerungen des Laguerreschen Satzes.

Wir werden die folgenden Verallgemeinerungen des Laguerreschen Satzes beweisen:

III. Ist $f(x)$ ein Polynom höchstens n-ten Grades und ist ξ eine beliebige Stelle der x-Ebene, für die $f(\xi) \neq 0$ und $f'^2(\xi) - f(\xi) \cdot f''(\xi) \neq 0$ ist, so liegt mindestens eine Nullstelle von $f(x)$ im Innern oder am Rande einer jeden Bernoullischen Lemniskate, die durch die beiden Punkte $\xi \mp \frac{\sqrt{n} \cdot f(\xi)}{\sqrt{f'^2(\xi) - f(\xi)\, f''(\xi)}}$ hindurchgeht und den Doppelpunkt ξ hat. Liegen nicht alle Nullstellen von $f(x)$ auf dem Rande der Ovale einer solchen Lemniskate, so hat das Polynom $f(x)$ Nullstellen innerhalb und auch außerhalb der Gebiete der Ovale.

IV. *Es sei $f(x)$ ein Polynom, es sei ξ eine beliebige Stelle der komplexen x-Ebene, für die $f(\xi) \neq 0$ und $f'^2(\xi) - f(\xi) \cdot f''(\xi) \neq 0$ ist, und es sei W_ξ ein Scheitelwinkelraum der x-Ebene, dessen Scheitel der Punkt ξ ist, dessen Schenkel g_1 und g_2 senkrechte Geraden sind und dessen Inneres die Punkte $\xi - \eta$ und $\xi + \eta$ enthält, wo $\eta = \frac{f(\xi)}{\sqrt{f'^2(\xi) - f(\xi) \cdot f''(\xi)}}$ ist. Liegen nun höchstens p Nullstellen von $f(x)$ im Inneren des Winkelraumes W_ξ, so liegt mindestens eine Nullstelle von $f(x)$ im Inneren oder am Rande der Bernoullischen Lemniskate, die durch die Punkte $\xi - \sqrt{p}\,\eta$ und $\xi + \sqrt{p}\,\eta$ hindurchgeht und die den Doppelpunkt ξ und in diesem Doppelpunkte die Tangenten g_1 und g_2 hat. Liegen alle Nullstellen von $f(x)$, die im Innern des Winkelraumes W_ξ sind, auf der Lemniskate, so liegen die übrigen Nullstellen von $f(x)$ alle auf den Geraden g_1 und g_2.*

Aus der Gleichung (2) erhält man durch Differentiation nach ξ die Gleichung

$$\frac{[f'(\xi)]^2 - f(\xi) \cdot f''(\xi)}{f^2(\xi)} = \sum_{k=1}^{n} \frac{1}{(\alpha_k - \xi)^2}. \tag{7}$$

Sind $\alpha_h - \xi = r_h\, e^{i\psi_h} = r_h \cdot e^{i(\varphi_h + \omega)}$ $(h = 1, 2, \ldots, n)$ und

$$\frac{f^2(\xi)}{f'^2(\xi) - f(\xi) \cdot f''(\xi)} = R^2 \cdot e^{2i\psi} = R^2 \cdot e^{2i(\varphi + \omega)},$$

wo ω einen beliebigen Winkel bedeutet, für den $\cos 2\varphi = \cos 2(\psi - \omega) > 0$ ist, so besteht für den reellen Teil der mit $e^{2i\omega}$ multiplizierten Gleichung (7) die Gleichung

---

[4]) Vgl. die Sätze des Verfassers in Jahresbericht d. DMV. **27** (1918), S. 44—48, in Tôhoku math. Journal **35** (1932), S. 126—135 und in Mat. és Fiz. Lapok **38** (1931), 41—60.

$$\frac{\cos 2\varphi}{R^2} = \sum_{k=1}^{n} \frac{\cos 2\varphi_k}{r_k^2}. \tag{8}$$

Hat die rechte Seite der Gleichung (8) p positive Glieder, unter denen $\frac{\cos 2\varphi_1}{r_1^2}$ am größten ist, so besteht die Ungleichung

$$p\,\frac{\cos 2\varphi_1}{r_1^2} \geqq \frac{\cos 2\varphi}{R^2} = \frac{1}{A^2} \text{ oder } r_1^2 \leqq p\,A^2 \cos 2\varphi_1. \tag{9}$$

Diese Ungleichung drückt unseren Satz IV aus, sie besteht mit dem Gleichheitszeichen nur dann, wenn die rechte Seite von (8) p positive gleiche Glieder hat und ihre übrigen Glieder alle verschwinden. In diesem Falle liegen p Nullstellen von $f(x)$ auf der Lemniskate $r^2 = p\,A^2 \cos 2\varphi$, die übrigen Nullstellen liegen auf den Geraden g_1 und g_2.

Aus dem Satze IV folgt der Satz III.

Kennt man einige Nullstellen von $f(x)$, so kann man aus der Gleichung (8) für die Lage der übrigen Nullstellen auch andere Ungleichungen ableiten.

Aus der Gleichung (2) erhält man durch $(q\text{-}1)$-malige Differentiation nach ξ die Gleichung

$$-\frac{1}{(q-1)!}\left[\frac{f'(\xi)}{f(\xi)}\right]^{(q-1)} = F(\xi) = \sum_{k=1}^{n} \frac{1}{(\alpha_k - \xi)^q} \tag{10}$$

Setzt man $\alpha_k - \xi = r_k \cdot e^{i\psi_k} = r_k \cdot e^{i(\varphi_k+\omega)}$ und $F(\xi) = R^q \cdot e^{qi\psi} = R^q \cdot e^{qi(\varphi+\omega)}$, wo ω einen beliebigen Winkel bedeutet, für den $\cos q\varphi = \cos q(\psi - \omega) > 0$ ist, so besteht für den reellen Teil der mit $e^{qi\omega}$ multiplizierten Gleichung (10) die folgende Relation

$$\frac{\cos q\ \varphi}{R^q} = \sum_{k=1}^{n} \frac{\cos q\,\varphi_k}{r_k^q} \tag{11}$$

Die rechte Seite dieser Gleichung hat wenigstens ein positives Glied. Ist $\frac{\cos q\,\varphi_1}{r_1^q}$ das größte positive Glied der rechten Seite von (11) und ist p die Anzahl der positiven Glieder, so besteht die Ungleichung

$$p\,\frac{\cos q\,\varphi_1}{r_1^q} \geqq \frac{\cos q\,\varphi}{R^q} = \frac{1}{A^q} \text{ oder } r_1^q \leqq pA^q \cos q\,\varphi_1\,. \tag{12}$$

Eine Kurve, die in polaren Koordinaten $(r,\ \varphi)$ die Gleichung $r^q = a^q \cos q\,\varphi$ hat, ist eine Sinusspirale vom Index q. Ist $q = 1$ oder 2, so ist die Kurve ein Kreis bzw. eine Bernoullische Lemniskate. Ist q eine ganze positive Zahl, so ist der Pol $r = 0$ ein q-facher Punkt mit q verschiedenen Tangenten, durch die der volle Winkel in $2q$ gleiche Winkel geteilt wird. Die Kurve besteht aus q kongruenten Ovalen, die in q nicht benachbarten Winkelräumen der $2q$ Winkel liegen und in dem q-fachen Punkte $r = 0$ miteinander zusammenhängen.

Aus der Ungleichung (12) folgen also die Sätze:

V. *Es sei $f(x)$ ein Polynom höchstens n-ten Grades und ξ eine beliebige Stelle der komplexen x-Ebene, für die $f(\xi)$ und $-\frac{1}{(q-1)!}\left[\frac{f'(\xi)}{f(\xi)}\right]^{(q-1)} = F(\xi)$ von Null verschieden sind, so liegt mindestens eine Nullstelle von $f(x)$ im Innern oder am Rande der q Ovale der Sinusspirale vom Index q, die im Punkte ξ den Mittelpunkt hat und die durch die q Punkte $\xi + e^{\frac{2k\pi}{q}i}\left[\frac{n}{F(\xi)}\right]^{\frac{1}{q}}$ $(k = 0, 1, \ldots, q-1)$ hindurchgeht. Liegen nicht alle Nullstellen von $f(x)$ auf dem Rande der q Ovale, so hat $f(x)$ Nullstellen innerhalb und auch außerhalb der Ovale.*

VI. *Es sei $f(x)$ ein Polynom und ξ eine beliebige Stelle der x-Ebene, für die $f(\xi)$ und* $-\frac{1}{(q-1)!}\left[\frac{f'(\xi)}{f(\xi)}\right]^{(q-1)} = F(\xi)$ *von Null verschieden sind. Es seien $g_1, g_2, \ldots, g_q$ solche Geraden durch den Punkt ξ, durch die der volle Winkel um den Punkt ξ in $2q$ gleiche Winkelräume geteilt wird. Liegen nun höchstens p Nullstellen von $f(x)$ in den q nicht benachbarten Winkelräumen von der Öffnung $\frac{\pi}{q}$, in denen die q Punkte*

$$\xi + e^{\frac{2k\pi}{q}i}\left[\frac{1}{F(\xi)}\right]^{\frac{1}{q}} = \xi + e^{\frac{2k\pi}{q}i}\cdot\eta \qquad (k = 0, 1, \ldots, q-1)$$

liegen, so liegt mindestens eine Nullstelle von $f(x)$ im Innern oder am Rande der Sinusspirale vom Index q, die im Punkte ξ einen q-fachen Punkt mit den Tangenten $g_1, g_2, \ldots, g_q$ hat und die durch die q Punkte $\xi + e^{\frac{2k\pi}{q}i}\sqrt[q]{p}\cdot\eta$ hindurchgeht.

4. Anwendungen.

Wendet man den Satz III im Falle $\xi = 0$ auf die Gleichung

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0 \tag{13}$$

an, so erhält man die folgenden Sätze:

VII. *Ist $a_0(a_1^2 - 2a_0a_2) \neq 0$, so liegt mindestens eine Wurzel der Gleichung*

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

im Innern oder am Rande einer jeden Bernoullischen Lemniskate, die durch die Punkte $\pm\sqrt{\frac{na_0^2}{a_1^2 - 2a_0a_2}}$ *hindurchgeht und den Doppelpunkt $x = 0$ hat. Liegt keine Wurzel der Gleichung im Innern einer solchen Lemniskate, so liegen alle Wurzeln der Gleichung auf der betreffenden Lemniskate.*

VIII. *Die Gleichung*

$$1 - x^2 + a_3x^3 + a_4x^4 + \cdots + a_nx^n = 0 \qquad (n > 2) \tag{14}$$

hat wenigstens eine Wurzel im Innern oder am Rande der Lemniskate $r^2 = \frac{n}{2}\cos 2\varphi$. Sie hat mindestens eine Wurzel auch im Innern oder am Rande einer jeden Bernoullischen Lemniskate, die den Punkt $x = 0$ zum Doppelpunkt hat, und die durch die Punkte $+\sqrt{\frac{n}{2}}$ *und* $-\sqrt{\frac{n}{2}}$ *hindurchgeht. Liegt keine Wurzel der Gleichung im Innern einer solchen Lemniskate, so liegen alle Wurzeln der Gleichung auf der betreffenden Lemniskate.*

Nach einem Satze von L. Fejér [5]) enthält der Kreis, der die Strecke von Null bis $+\sqrt{\frac{n(n-1)}{2}}$ oder bis $-\sqrt{\frac{n(n-1)}{2}}$ zum Durchmesser hat, mindestens eine Nullstelle der Gleichung (14). Der Satz VIII gibt also ein wesentlich kleineres Gebiet für eine Wurzel der Gleichung (14). Der Flächeninhalt dieses Gebiet ist $\frac{\pi}{4}(n-1)$-mal kleiner, als der eines Fejérschen Kreises.

Wendet man den Satz V im Falle $\xi = 0$ auf die Gleichung (13) an, so erhält man auch andere Sätze. So bestehen z. B. die folgenden Sätze:

---

[5]) Jahresbericht d. DMV. **26** (1917), S. 127.

IX. *Die Gleichung*

$$1 - x^q + a_{q+1}x^{q+1} + a_{q+2}x^{q+2} + \cdots + a_n x^n = 0 \qquad (q \geqq 2) \tag{15}$$

hat mindestens eine Wurzel im Innern oder am Rande der q Ovale der Sinusspirale $r^q = \frac{n}{q}\cos q\varphi$. *Enthält keines dieser Ovale im Innern Wurzeln der Gleichung, so liegen ihre Wurzeln alle auf der Sinusspirale.*

X. *Die Gleichung*

$$1 + e^{i\gamma}x^q + a_{q+1}x^{q+1} + a_{q+2}x^{q+2} + \cdots + a_n x^n = 0 \qquad (q \geqq 2), \tag{16}$$

wo der Winkel γ beliebig ist, hat mindestens eine Wurzel im Kreise $|x| = \sqrt[q]{\frac{n}{q}}$.

Kennt man in der Koeffizientenfolge $e^{i\gamma}$, a_{q+1}, a_{q+2}, . . ., a_n keine Lücken, so kann man nach einem Satze von L. Fejér[6]) behaupten, daß der Kreis $|x| = \sqrt[q]{\binom{n}{q}}$ mindestens zwei Wurzeln von (16) enthält. (Dieser Kreis enthält nach einer Vermutung von P. Montel, die von E. B. Van Vleck für Gleichungen (16) ohne Lücken und von M. Biernacki für Gleichungen (16) mit Lücken bewiesen wurde, mindestens q Wurzeln von (16)[7]).

Dieser Kreis, der mindestens eine Wurzel von (16) enthält, hat einen $\sqrt[q]{\binom{n-1}{q-1}}$-mal kleineren Halbmesser, als der vorige Kreis.

Die Sätze VII, VIII, IX und X lassen sich im allgemeinen nicht verschärfen, wie aus den Gleichungen

$$\left(1 - \frac{2}{n}\cdot x^2\right)^{\frac{n}{2}} = 1 - x^2 + a_4 x^4 + \cdots + a_n x^n = 0$$

bzw.

$$\left(1 - \frac{q}{n}x^q\right)^{\frac{n}{q}} = 1 - x^q + a_{2q}x^{2q} + \cdots + a_n x^n = 0$$

$$\left(1 + e^{\frac{\gamma}{n}i}\,\frac{q}{n}\,x^q\right)^{\frac{n}{q}} = 1 + e^{\gamma i}x^q + \cdots + a_n x^n = 0$$

hervorgeht, wo n eine gerade bzw. eine durch q teilbare Zahl bedeutet. Diese Gleichungen haben keine Wurzel im Innern der von dem betreffenden Satz bestimmten Gebiete, ihre Wurzeln liegen alle auf dem Rande der betreffenden Gebiete.

Ist $p = 2k$ eine gerade Zahl und sind $\gamma_1, \gamma_2, \ldots, \gamma_m$ reelle Zahlen, deren Summe Null ist, so hat die Gleichung

$$f(x) = \left(1 - \frac{2}{p}x^2\right)^{\frac{p}{2}}(1 + i\gamma_1 x^2)(1 + i\gamma_2 x^2)\ldots(1 + i\gamma_m x^2) = 0 \qquad (i = \sqrt{-1})$$

p Wurzeln auf der Lemniskate $r^2 = \frac{p}{2}\cos 2\varphi$, ihre übrigen Wurzeln liegen alle auf den Tangenten des Doppelpunktes dieser Lemniskate. Daraus folgt, daß der Satz IV (im Falle $\xi = 0$) sich nicht verschärfen läßt.

5. Nachträgliche Anmerkungen.

Während der Korrektur[8]) habe ich den folgenden Satz von R. D. Carmichael und Mason[9]) bemerkt:

---

[6]) u. [7]) Vgl. die in der Fußnote [3]) zitierten Arbeiten.

[8]) 20. Jan. 1933.

[9]) Bull. of. the Amer. Math. Soc. **21** (1914—1915), S. 14—22.

Jede algebraische Gleichung von der Form

$$1 + x^p + a_{sq+1}x^{sq+1} + a_{sq+2}x^{sq+2} + \cdots + a_n x^n = 0 \qquad (s \geqq 1)$$

hat mindestens eine Wurzel, deren absoluter Betrag nicht größer als $\sqrt[sq]{\frac{n}{q}}$ *ist.*

Der Satz *X* ist eine leichte Folgerung dieses Satzes.

Es gilt auch der folgende Satz:

XI. *Jede algebraische Gleichung von der Form*

(17) $$1 - x^p + a_{sq+1}x^{sq+1} + a_{sq+2}x^{sq+2} + \cdots + a_n x^n = 0 \qquad s \geqq 1$$

hat mindestens eine Wurzel im Innern oder am Rande der Ovale der Sinusspirale, deren Gleichung in Polarkoordinaten $r^{sq} = \frac{n}{q}\cos sq\varphi$ *ist. Enthält keines dieser Ovale im Innern eine Wurzel der Gleichung, so liegen ihre Wurzeln alle auf der Sinusspirale.*

Dieser Satz folgt aus dem Satz V, wenn man q durch sq und ξ durch Null ersetzt. In diesem Falle ist

$$F(\xi) = -\frac{1}{(sq-1)!}\left[\frac{f'(\xi)}{f(\xi)}\right]^{(sq-1)} = \sum \frac{1}{(\alpha_k - \xi)^{sq}} \text{ und } F(0) = \sum \frac{1}{\alpha_k^{sq}}.$$

Sind $\beta_1, \beta_2, \ldots, \beta_n$ die Wurzeln der Gleichung

$$A_0 + A_1 x + A_2 x^2 + \cdots + A_n x^n = 0$$

und bezeichnet S_m die Potenzsumme $\sum \frac{1}{\beta_k^m}$ $(m > 0)$, so bestehen die bekannten Newtonschen Formeln

$$S_m + A_1 \cdot S_{m-1} + A_2 \cdot S_{m-2} + \cdots + A_{m-1} \cdot S_1 + m.\ A_m = 0 \quad (m = 1, 2, \ldots).$$

Im Falle der Gleichung (17) sind $A_0 = 1$, $A_1 = A_2 = \cdots = A_{q-1} = 0$, $A_q = -1$, $A_{q+1} = A_{q+2} = \cdots = A_{sq} = 0$. Daraus folgt, daß

$$S_q = S_{2q} = \cdots = S_{sq} = q = \sum \frac{1}{\alpha_k^{sq}}$$

sind. Damit ist der Satz XI bewiesen.

Auch im Falle $\xi \neq 0$ und für jedes Polynom $f(x)$ n-ten Grades läßt sich der Wert $F(\xi)$ durch die Formel der Newtonschen Potenzsummen bestimmen. Sind nämlich $\alpha_1, \alpha_2, \ldots, \alpha_n$ die Nullstellen des Polynoms $f(x)$, so sind

$$\beta_1 = \alpha_1 - \xi,\ \beta_2 = \alpha_2 - \xi, \ldots, \beta_n = \alpha_n - \xi$$

die Nullstellen des Polynoms

$$P(z) = f(\xi + z) = f(\xi) + \frac{f'(\xi)}{1!}z + \frac{f''(\xi)}{2!}z^2 + \cdots + \frac{f^{(n)}(\xi)}{n!}z^n.$$

Daraus folgt, daß

$$-\frac{1}{(q-1)!}\left[\frac{f'(\xi)}{f(\xi)}\right]^{(q-1)} = \sum \frac{1}{(\alpha_k - \xi)^q} = \sum \frac{1}{\beta_k^q} = s_q$$

und

$$f(\xi) \cdot S_q + \frac{f'(\xi)}{1!}S_{q-1} + \frac{f''(\xi)}{2!}S_{q-2} + \cdots + \frac{f^{(q-1)}(\xi)}{(q-1)!}S_1 + q\frac{f^{(q)}(\xi)}{q!} = 0$$

sind.

Eingegangen 30. Juni 1932.

Dr. Clemens Schaefer
o. ö. Prof. a. d. Univ. Breslau

Einführung in die theoretische Physik

I. Band. 3. Auflage. Mit 272 Figuren. XII, 991 Seiten. 1929. RM 45.—, geb. 48.—

II. Band. 2. Auflage. Mit 88 Figuren. X, 660 Seiten. 1929. RM 28.—, geb. 30.—

III. Band, 1. Teil: Elektrodynamik und Optik. Mit 235 Figuren im Text. VIII, 918 Seiten. 1932. RM. 37.50, geb. 40.—

Der zweite Teil des dritten Bandes enthält die Quantentheorie und erscheint im Herbst 1933.

Zeitschrift d. mathemat. u. naturwissenschaftl. Unterrichts
„Das Buch füllt gewiß eine empfindliche Lücke in unserer Lehrbuchliteratur für den Hochschulunterricht aus. Es stellt den letzten Stand der Wissenschaft dar und kann wegen seiner Klarheit und daher seiner verhältnismäßig leichten Lesbarkeit, auch seines reichen Inhalts wegen angelegentlich empfohlen werden."

Monatshefte für Mathematik und Physik
„Die ersten Kapitel bewegen sich naturgemäß großenteils auf klassischem Boden, die Darstellung ist aber durchaus modern und die Fassungen überall *von mustergültiger Klarheit.*"

Ein ausführlicher Sonderprospekt steht kostenlos zur Verfügung.

Walter de Gruyter & Co., Berlin W 10
Genthiner Straße 38

Soeben erschienen:

Algebra

Von Dr. **Oskar Perron,** o. ö. Professor der Mathematik an der Universität München.

II. Theorie der algebraischen Gleichungen

Zweite, verbesserte Auflage. Mit 5 Figuren. Groß-Oktav. VIII, 261 Seiten. Geb. RM 9.50

(Göschens Lehrbücherei. 1. Gruppe: Reine und angewandte Mathematik, Band 9).

Mit dem jetzt erscheinenden zweiten Band ist die zweite, verbesserte Auflage abgeschlossen. Der erste Band, „Die Grundlagen", geb. RM 11.50, gelangte im März v. Jhrs. zur Ausgabe. Wie dieser Band, so hat auch der zweite Band erhebliche Änderungen erfahren. Das erste Kapitel wurde stark erweitert. Die Kapitel 3 und 4 sind erheblich umgearbeitet und durch Hinzunahme einiger früher weggelassener Dinge erheblich erweitert. Dagegen sind die Kapitel 2 und 5 nur wenig geändert worden.

Geschichte der Elementar-Mathematik

in systematischer Darstellung mit besonderer Berücksichtigung der Fachwörter.

Von Dr. **Johannes Tropfke,** Oberstudiendirektor an der Kirschner-Schule zu Berlin.

II. Band: Allgemeine Arithmetik

Dritte, verbesserte und vermehrte Auflage. Groß-Oktav. IV, 266 Seiten. RM 12.—, geb. 13.50

Nachdem in dritter Auflage der erste Band im Jahre 1930 zur Ausgabe gelangte, folgt jetzt der zweite Band, der die allgemeine Arithmetik behandelt. Das Gesamtwerk bringt die Geschichte der Elementarmathematik in systematischer Anordnung und in zusammenhängender Darstellung unter peinlich genauer Zitierung der Quellen (bis in die neueste Zeit). Es ist grundlegend für den, der sich einen allgemeinen Überblick verschaffen will, unentbehrlich aber auch für den, der sich mit der Geschichte der Mathematik in Spezialstudien befaßt. Die weiteren Bände sind in Vorbereitung.

Walter de Gruyter & Co., Berlin W 10 Genthiner Str. 38

Diesem Heft liegt ein Prospekt der Verlagsbuchhandlung Friedr. Vieweg & Sohn in Braunschweig bei.